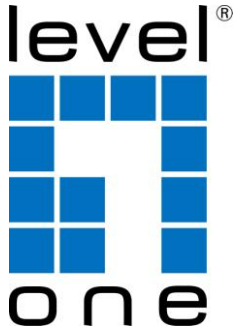


LevelOne

WAP-6002

150Mbps *N* Wireless Access Point

User Manual

V1.0.0

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION 1
- **Features of your Wireless Access Point** 1
- **Package Contents** 3
- **Physical Details** 3

CHAPTER 2 INSTALLATION 6
- **Requirements** 6
- **Procedure** 6

CHAPTER 3 ACCESS POINT SETUP 7
- **Overview** 7
- **Setup using a Web Browser** 7
- **Setup Wizard** 9
- **Wireless Setting Screens** 10
- **Wireless Mode Screen** 12
- **MAC Filter** 25
- **Wi-Fi Protected Setup** 28

CHAPTER 4 PC AND SERVER CONFIGURATION 29
- **Overview** 29
- **Using WEP** 29
- **Using WPA-PSK/WPA2-PSK** 30
- **802.1x Server Setup (Windows 2000 Server)** 31
- **802.1x Client Setup on Windows XP** 41
- **Using 802.1x Mode (without WPA)** 47

CHAPTER 5 ACCESS POINT MANAGEMENT 48
- **Overview** 48
- **Status Screen** 48
- **Password Screen** 50
- **Config File** 51
- **Firmware Upgrade** 52

APPENDIX A SPECIFICATIONS 53
- **Wireless Access Point** 53

APPENDIX B TROUBLESHOOTING 56
- **Overview** 56
- **General Problems** 56

APPENDIX C WINDOWS TCP/IP 58
- **Overview** 58
- **Checking TCP/IP Settings - Windows 9x/ME:** 58
- **Checking TCP/IP Settings - Windows NT4.0** 60
- **Checking TCP/IP Settings - Windows 2000** 62
- **Checking TCP/IP Settings - Windows XP** 64
- **Checking TCP/IP Settings - Windows Vista/7** 66

APPENDIX D ABOUT WIRELESS LANS 68
- **Overview** 68
- **Wireless LAN Terminology** 68

Copyright © 2009. All Rights Reserved.

All trademarks and trade names are the properties of their respective owners.

Chapter 1
Introduction

This Chapter provides an overview of the Wireless Access Point's features and capabilities.

Congratulations on the purchase of your new Wireless Access Point. The Wireless Access Point links your Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection.

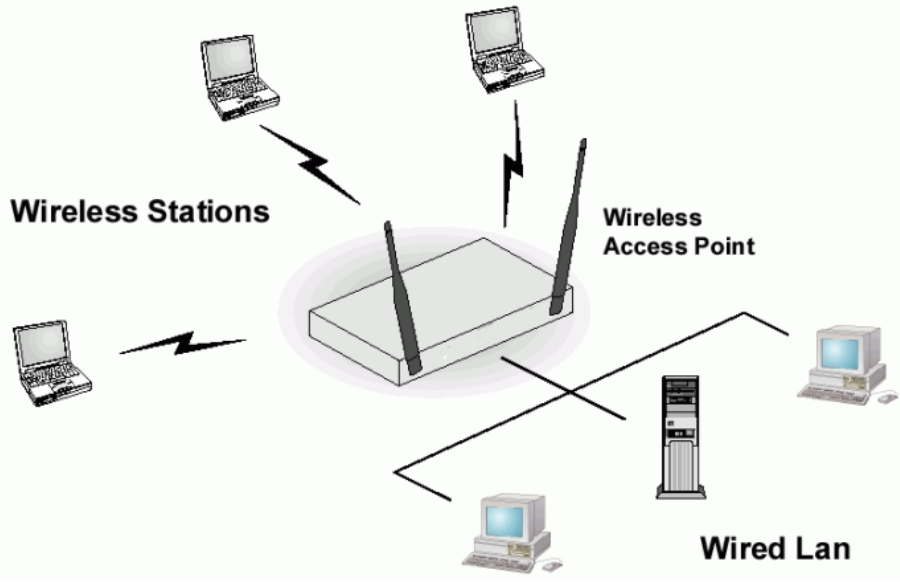


Figure 1: Wireless Access Point

The auto-sensing capability of the Wireless Access Point allows packet transmission up to 300Mbps for maximum throughput, or automatic speed reduction to lower speeds when the environment does not permit maximum throughput.

Features of your Wireless Access Point

The Wireless Access Point incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

- ***Standards Compliant.*** The Wireless Access Point complies with the IEEE802.11g and IEEE802.11n 2.0 specifications for Wireless LANs.
- ***Supports 11n Wireless Stations.*** The 802.11n standard provides for backward compatibility with the 802.11b standard, so 802.11n, 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***Bridge Mode Support.*** The Wireless Access Point can operate in Bridge Mode, connecting to another Access Point. Both PTP (Point to Point) and PTMP (Point to Multi-Point) Bridge modes are supported.
  And you can even use both Bridge Mode and Access Point Mode simultaneously!

WPS Support. WPS (Wi-Fi Protected Setup) can simplify the process of connecting any device to the wireless network by using the push button configuration (PBC) on the Wireless Access Point, or entering PIN code if there's no button.

- ***DHCP Client Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Access Point can act as a **DHCP Client**, and obtain an IP address and related information from your existing DHPC Server.
- ***Upgradeable Firmware.*** Firmware is stored in a flash memory and can be upgraded easily, using only your Web Browser.

Security Features

- ***Virtual APs.*** For maximum flexibility, wireless security settings are stored in Virtual AP. Up to 7 Virtual APs can be defined and used as any time.
- ***Multiple SSIDs.*** Because each Virtual AP has it own SSID and beacon, and up to 7 Virtual APs can be active simultaneously, multiple SSIDs are supported. Different clients can connect to the Wireless Access Point using different SSIDs, with different security settings.
- ***Virtual APs Isolation.*** If desired, PCs and devices connecting to different Virtual APs can be isolated from each other.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Both 64 Bit 128 Bit, and 152 Bit keys are supported.
- ***WPA support.*** Support for WPA is included. WPA is more secure than WEP, and should be used if possible. Both TKIP and AES encryption methods are supported.
- ***802.1x Support.*** Support for 802.1x mode is included, providing for the industrial-strength wireless security of 802.1x authentication and authorization.
- ***Radius Client Support.*** The Wireless Access Point can login to your existing Radius Server (as a Radius client).
- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

Advanced Features

- ***SNMP Support.*** SNMP (Simple Network Management Protocol) is supported, allowing you to use a SNMP program to manage the Wireless Access Point.
- ***WDS Support***. Support for WDS (Wireless Distribution System) allows the Wireless Access Point to act as a Wireless Bridge. Both Point-to-Point and Multi-Point Bridge modes are supported.

Package Contents

The following items should be included:

- WAP-6002 150Mbps *N* Wireless Access Point
- Power Adapter
- Quick Start Guide
- CD-ROM containing the on-line manual and setup utility.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel LEDs

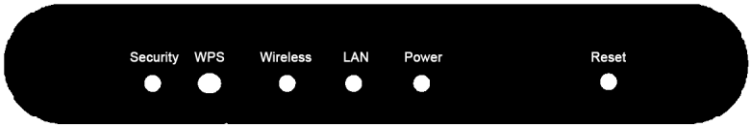


Figure 2: Front Panel

Security	**Off** - WPS feature is not in use.
	On (White) - If the LED is on for a while and then off, WPS is processing successfully.
	Blinking (White) - WPS feature is currently in use.
WPS Button	Push the WPS button on the device and on your other wireless device to perform WPS function that easily creates an encryption-secured wireless connection automatically.
Wireless	**On** - Idle
	Off - Wireless connection is not available.
LAN	**On** - The LAN port is active.
	Off - No active connection on the LAN (Ethernet) port.
Power	**On** - Normal operation.
	Off - No power

Reset Button

This button has two (2) functions:

- **Reboot**. When pressed and released, the Wireless Access Point will reboot (restart).
- **Reset to Factory Defaults**. This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To Clear All Data and restore the factory default values:

1. Hold the Reset Button for more than 5 seconds.
2. Release the Reset Button.
   The factory default configuration has now been restored, and the Access Point is ready for use.

Rear Panel

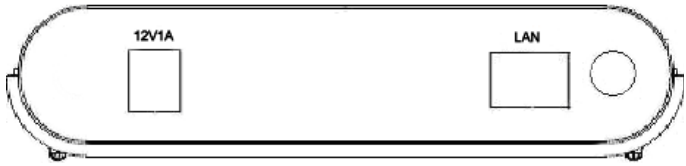


Figure 3: Rear Panel

or

Figure 4: Rear Panel

LAN	Use a standard LAN cable (RJ45 connectors) to connect this port to a 10BaseT or 100BaseT hub/switch on your LAN.
Power port	Connect the supplied power adapter (12V@1A) here.
Antenna	The antenna differs according to the different models.

Chapter 2
Installation

This Chapter covers the physical installation of the Wireless Access Point.

Requirements

Requirements:

- TCP/IP network
- Ethernet cable with RJ-45 connectors
- Installed Wireless network adapter for each PC that will be wirelessly connected to the network

Procedure

1. Select a suitable location for the installation of your Wireless Access Point. To maximize reliability and performance, follow these guidelines:
   - Use an elevated location, such as wall mounted or on the top of a cubicle.
   - Place the Wireless Access Point near the center of your wireless coverage area.
   - If possible, ensure there are no thick walls or metal shielding between the Wireless Access Point and Wireless stations.

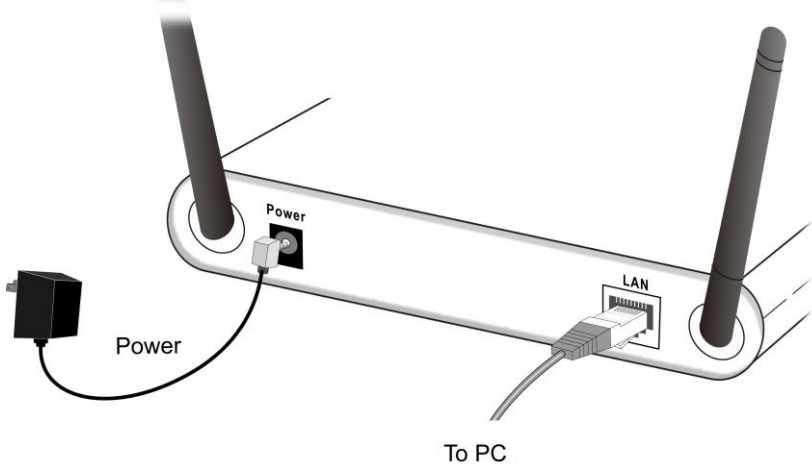


Figure 5: Installation Diagram

2. Use a standard LAN cable to connect the "LAN" port on the Wireless Access Point to a 10/100BaseT hub/switch on your LAN.
3. Connect the supplied power adapter to the Wireless Access Point and a convenient power outlet, and power up.
4. Check the LEDs:
   - The *Power* LED should be ON.
   - The *LAN* and *Wireless* LEDs should be ON.

   For more information, refer to *Front Panel LEDs* in Chapter 1.

Chapter 3
Access Point Setup

This Chapter provides details of the Setup process for Basic Operation of your Wireless Access Point.

Overview

This chapter describes the setup procedure to make the Wireless Access Point a valid device on your LAN, and to function as an Access Point for your Wireless Stations.

Wireless Stations may also require configuration. For details, see *Chapter 4 - Wireless Station Configuration*.

The Wireless Access Point can be configured using your Web Browser.

Setup using a Web Browser

Your Browser must support JavaScript. The configuration program has been tested on the following browsers:

- MAC OS X/Linux
- Windows98SE/ME/2000(SP4)/XP SP2/Vista/7

Setup Procedure

Before commencing, install the Wireless Access Point in your LAN, as described previously.

1. Check the Wireless Access Point to determine its *Default Name*. This is shown on a label on the base or rear
2. Use a PC which is already connected to your LAN, either by a wired connection or another Access Point.
   - Until the Wireless Access Point is configured, establishing a Wireless connection to it may be not possible.
   - If your LAN contains a Router or Routers, ensure the PC used for configuration is on the same LAN segment as the Wireless Access Point.
3. Start your Web browser.
4. In the *Address* box, enter "HTTP://" and the IP Address of the 11N Wireless Access Point, as in this example, which uses the Wireless Access Point's default IP Address:

   `HTTP://192.168.0.1`
5. You should then see a login prompt, which will ask for a *User Name* and *Password*. Enter **`admin`** for the *User Name*, and **`password`** for the *Password*. These are the default values. The password can and should be changed. Always enter the current user name and password, as set on the *Admin Login* screen.

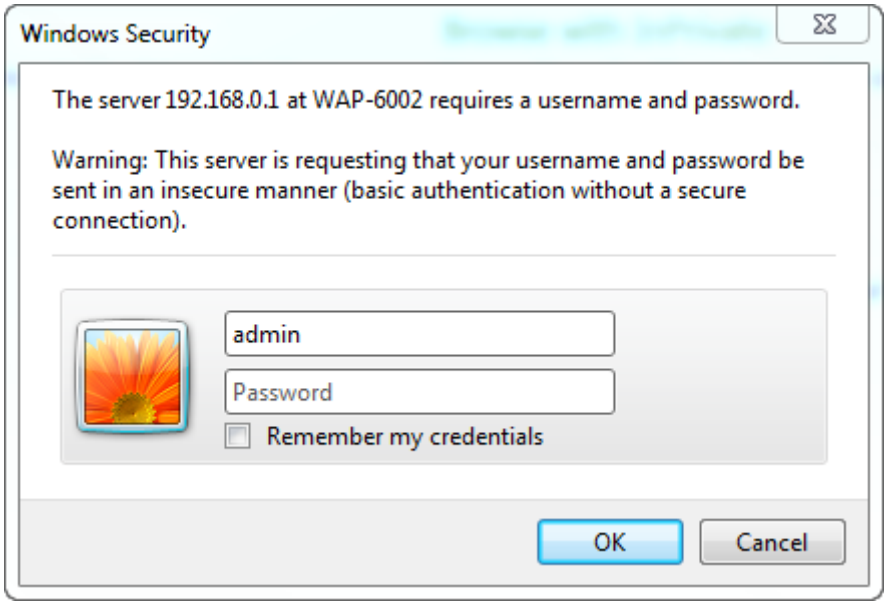

Windows Security
The server 192.168.0.1 at WAP-6002 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Password
Remember my credentials
OK
Cancel

Figure 6: Password Dialog

6. You will then see the *Home* screen, which displays the current settings and status. No data input is possible on this screen.

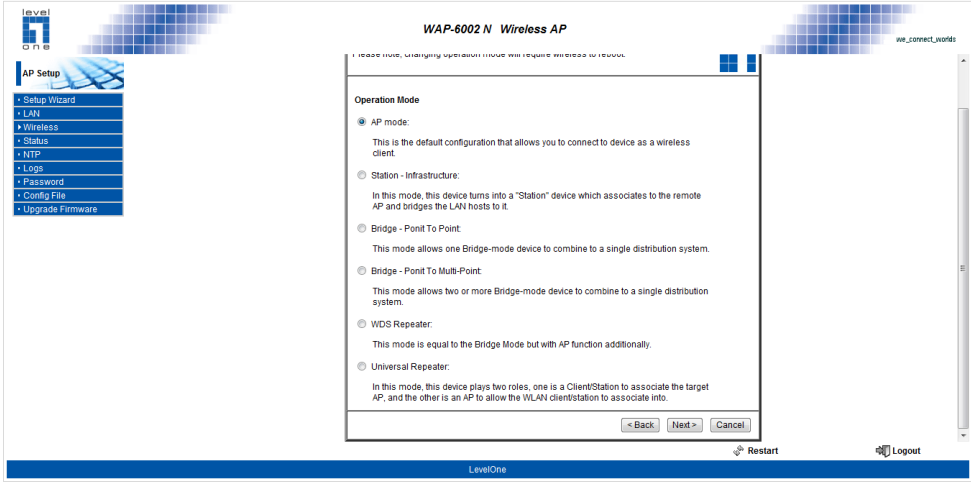

WAP-6002 N Wireless AP
AP Setup
Setup Wizard
LAN
Wireless
Status
NTP
Logs
Password
Config File
Upgrade Firmware
Operation Mode
AP mode:
This is the default configuration that allows you to connect to device as a wireless client.
Station - Infrastructure:
In this mode, this device turns into a "Station" device which associates to the remote AP and bridges the LAN hosts to it.
Bridge - Ponit To Point:
This mode allows one Bridge-mode device to combine to a single distribution system.
Bridge - Ponit To Multi-Point:
This mode allows two or more Bridge-mode device to combine to a single distribution system.
WDS Repeater:
This mode is equal to the Bridge Mode but with AP function additionally.
Universal Repeater:
In this mode, this device plays two roles, one is a Client/Station to associate the target AP, and the other is an AP to allow the WLAN client/station to associate into.
< Back
Next >
Cancel
Restart
Logout
LevelOne

Figure 7: Home Screen

7. From the menu, check the following screens, and configure as necessary for your environment. Details of these screens and settings are described in the following sections of this chapter.
8. You may also wish to set the admin password and administration connection options. These are on the *Password* screen accessed from the **main** menu.
9. Use the **Log Out** and **Restart** buttons on the menu to apply your changes and restart the Wireless Access Point.

Setup is now complete.

Wireless stations must now be set to match the Wireless Access Point. See Chapter 4 for details.

> **If you can't connect:**
>
> It is likely that your PC's IP address is incompatible with the Wireless Access Point's IP address. This can happen if your LAN does not have a DHCP Server. The default IP address of the Wireless Access Point is 192.168.0.1, with a Network Mask of 255.255.255.0.
>
> If your PC's IP address is not compatible with this, you must change your PC's IP address to an unused value in the range 192.168.0.1 ~ 192.168.0.254, with a Network Mask of 255.255.255.0. See ***Appendix C - Windows TCP/IP*** for details for this procedure.

Setup Wizard

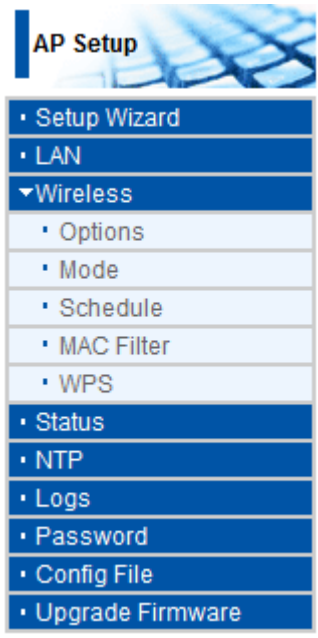
Click *Setup Wizard* in the main menu to help you simplify the configuration.

10. Step through the Wizard until finished.
    - You need to know the SSID and security settings used by the APs. Check the data carefully.
    - Refer to the Wireless Mode Screen for more details.
11. If the connection fails:
    - Check your data and all connections.
    - Check that you have entered all data correctly.

Wireless Setting Screens

The settings on this screen must match the settings used by Wireless Stations.

Click ***Wireless Setting*** on the main menu to view a screen like the following.



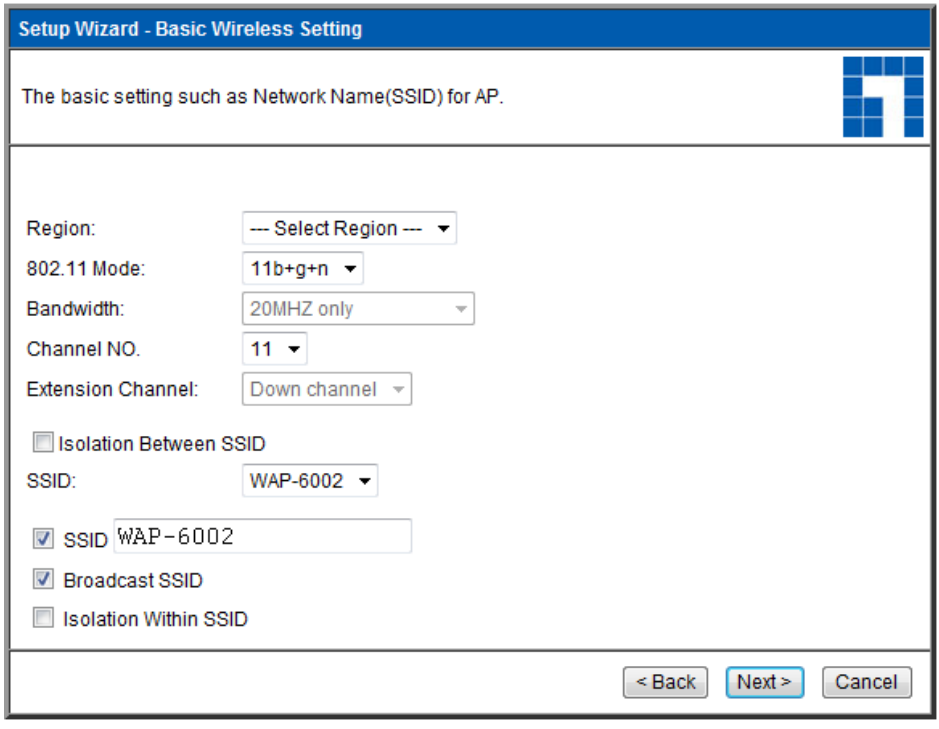


Figure 8:Wireless Setting Screen

Data - Wireless Setting Screen

Region	
Region	Select the country or domain matching your current location.
Options	
802.11 Mode	Select the desired option: • **Off** - select this if for some reason you do not this AP to transmit or receive at all. • **B only** - if selected, only 802.11b connections are allowed. 802.11g wireless stations will only be able to connect if they are fully backward-compatible with the 802.11b standard. • **G only** - only 802.11g connections are allowed. If you only have 802.11g, selecting this option may provide a performance improvement over using the default setting. • **11b/g/n** - this is the default, and will allow connections by 802.11n, 802.11b and 802.11g wireless stations.
Channel No	If "Automatic" is selected, the Access Point will select the best available Channel. If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with manually setting different channels to see which is the best.
Extension Channel	Select the desired option from the drop-down list.
Isolation between SSID	If Enabled, devices that have the different SSIDs will not be able to communicate with each other.
WMM Support	Enable or disable this feature as required.
Channel Bandwidth	Select the desired bandwidth from the list.

Wireless Mode Screen

Clicking the *Wireless Mode* link on the main menu will result in a screen like the following.

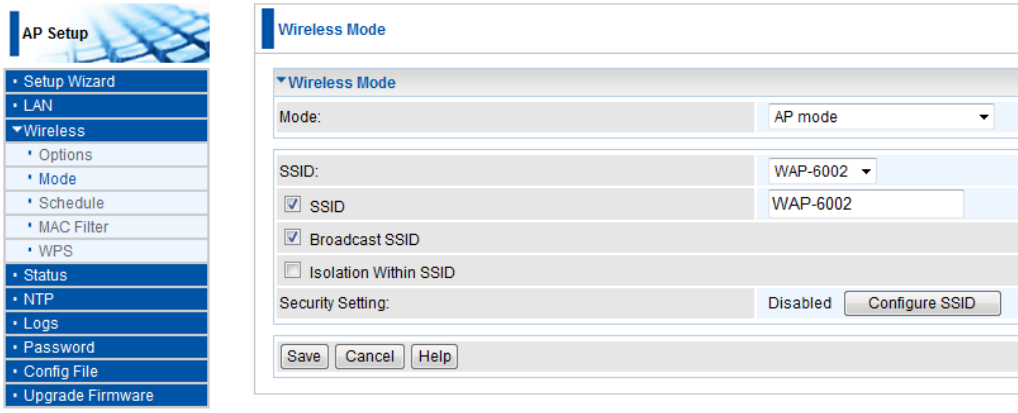


Figure 9: Wireless Mode Screen

Data - Wireless Mode Screen

Wireless Mode	
Mode	Select the desired mode: • **AP mode** - operate as a normal Access Point • **Station - Infrastructure -** Enter the SSID of the access point whose signal you would like to join or click on Site Survey to see a list of available access points. • **Bridge - Point-to-Point -** Bridge to a single AP. You must provide the MAC address of the other AP in the PTP Bridge AP MAC Address field. • **Bridge - Multi-Point -** Select this only if this AP is the "Master" for a group of Bridge-mode APs. The other Bridge-mode APs must be set to Point-to-Point Bridge mode, using this AP's MAC address. They then send all traffic to this "Master". • **WDS Repeate**r - act as a repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the **Remote AP MAC Address** field. In this mode, all traffic is sent to the specified AP. • **Universal Repeater** - act as an universal repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the **Remote AP MAC Address** field. In this mode, all traffic is sent to the specified AP.

AP Mode

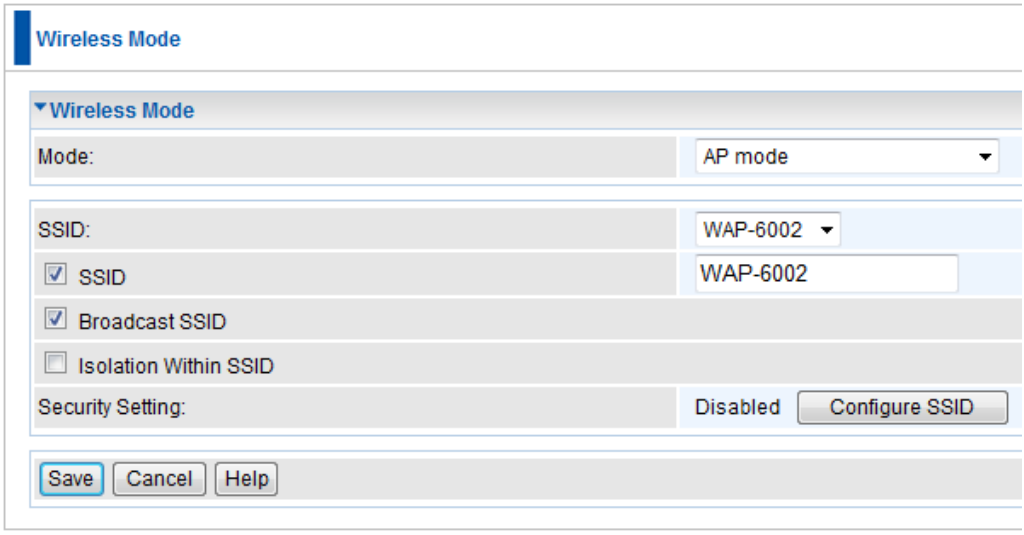


Figure 10: AP Mode

cd

AP Mode	
SSID	With Multiple SSIDs, you can have 2 SSIDs on one AP. For example, a Guest SSID without encryption for visitors to have Internet access only, and a Admin SSID with encryption for private use to secure your company resources. Select the desired SSID from the list to configure.
Broadcast SSID	If enabled, the Wireless ADSL Router will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID. If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.
Isolation within SSID	If Enabled, devices that have the same SSID will not be able to see each other.
Security Setting	The current Wireless security is displayed. The default value is Disabled.
Configure SSID Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.

Station - Infrastructure

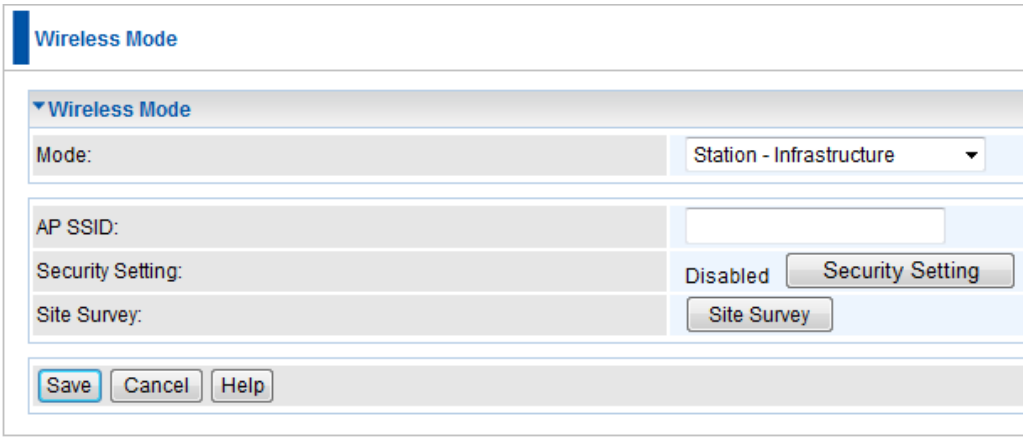


Figure 11: Station - Infrastructure

Station - Infrastructure	
AP SSID	Enter the desired SSID. Each profile must have a unique SSID.
Security Setting	The current Wireless security is displayed. The default value is Disabled. Click *Security Setting* button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
Site Survey	Click the *Site Survey* button to see a list of available access points.

Bridge - Point To Point

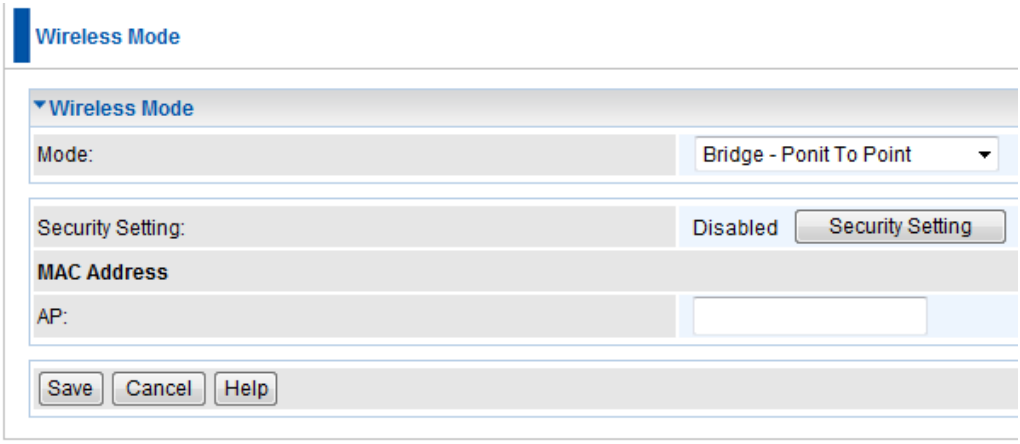


Figure 12: Bridge - Point To Point

Bridge - Point To Point	
Security Setting	The current Wireless security is displayed. The default value is Disabled. Click *Security Setting* button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
MAC Address	Enter the MAC address of the AP into the field to allow the following access point to be connected to the device.

Bridge - Point To Multi-Point

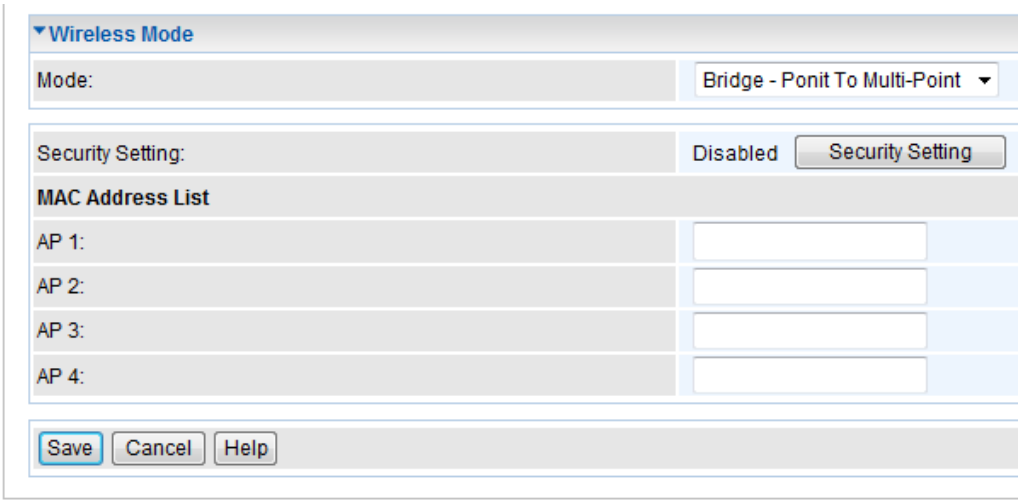


Figure 13: Bridge - Point To Multi-Point

Bridge - Point To Multi-Point	
Security Setting	The current Wireless security is displayed. The default value is Disabled. Click *Security Setting* button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
MAC Address List	Enter the MAC address(es) of the AP(s) into the fields to allow the following access points to be connected to the device.

WDS Repeater

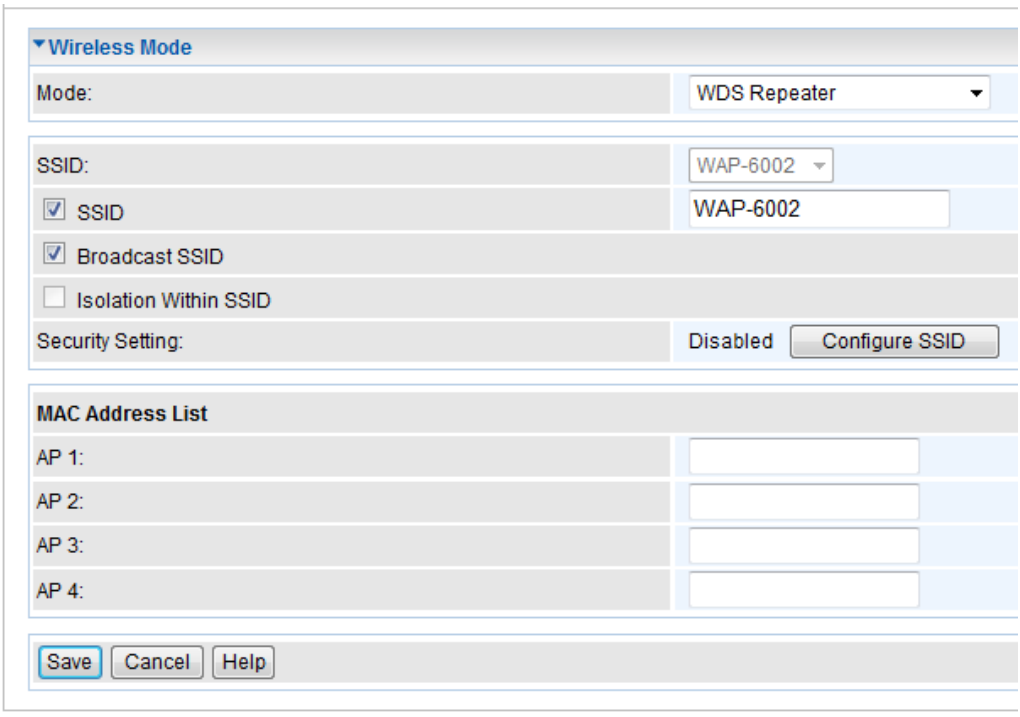


Figure 14: WDS Repeater

WDS Repeater	
SSID	Enter the desired SSID. Each Profile must have a unique SSID.
Broadcast SSID	If enabled, the Wireless ADSL Router will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID. If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.
Isolation within SSID	If Enabled, devices that have the same SSID will not be able to see each other.
Security Setting	The current Wireless security is displayed. The default value is Disabled.
Configure SSID Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
MAC Address List	Enter the MAC address(es) of the AP(s) into the fields to allow the following access points to be connected to the device.

Universal Repeater

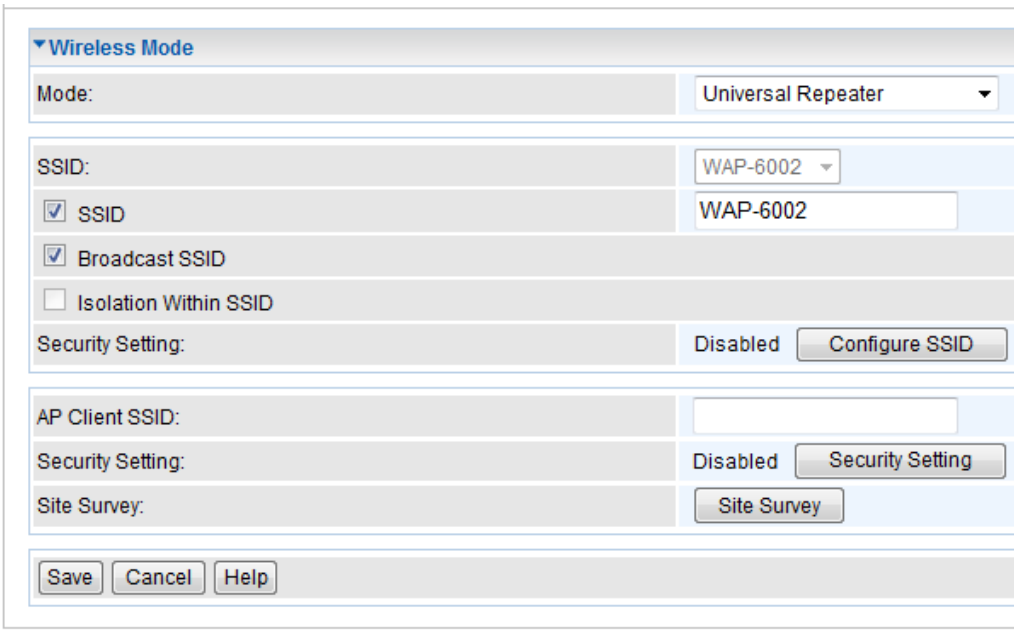


Figure 15: Universal Repeater

Universal Repeater	
SSID	Enter the desired SSID. Each Profile must have a unique SSID.
Broadcast SSID	If enabled, the Wireless ADSL Router will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID. If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.
Isolation within SSID	If Enabled, devices that have the same SSID will not be able to see each other.
Security Setting	The current Wireless security is displayed. The default value is Disabled.
Configure SSID Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
AP Client SSID	Enter the desired SSID. Each profile must have a unique SSID.
Security Setting	The current Wireless security is displayed. The default value is Disabled. Click *Security Setting* button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.

Security Settings

Select the desired option, and then enter the settings for the selected method.

The available options are:

- **None** - No security is used. Anyone using the correct SSID can connect to your network.
- **WEP** - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.
- **WPA-PSK** - Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- **802.1x** - This uses the 802.1x standard for client authentication, and WEP for data encryption.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must have a "user login" on the Radius Server.
  - Each user's wireless client must support 802.1x and provide the login data when required.
  - All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

Security Settings - None

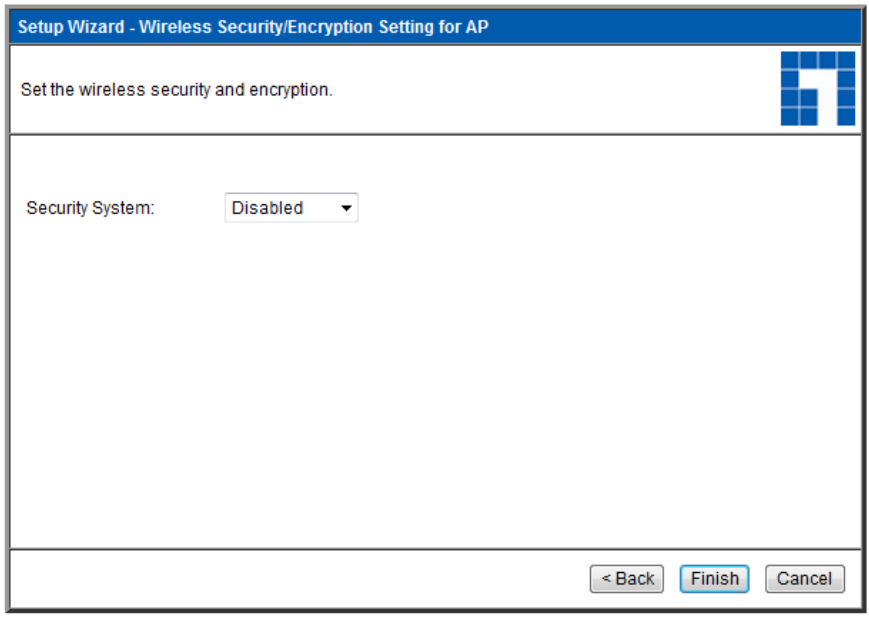


Figure 16: Wireless Security - None

No security is used. Anyone using the correct SSID can connect to your network.

Security Settings - WEP

This is the 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.

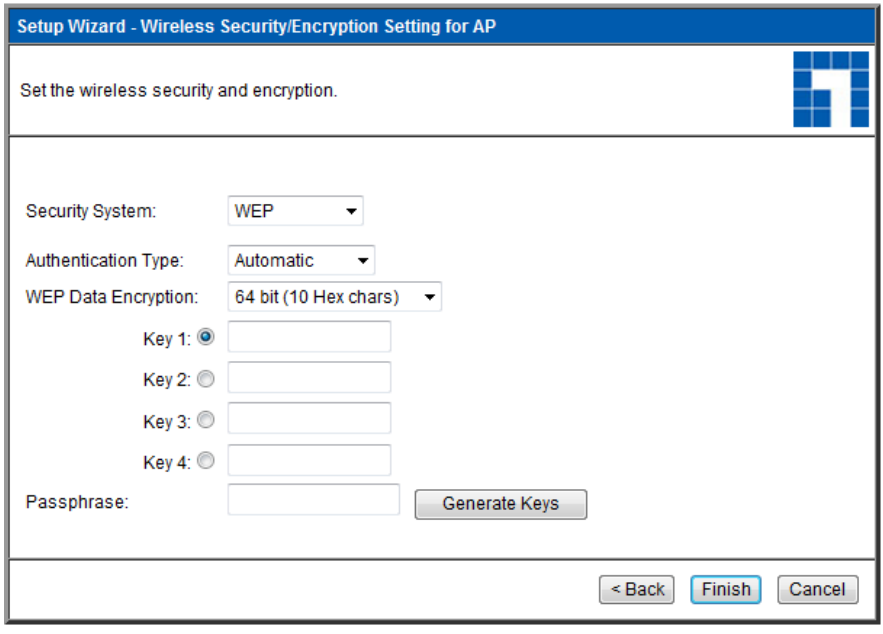


Figure 17: WEP Wireless Security Screen

Data - WEP Screen

WEP	
Authentication	Normally, you can leave this at “Automatic”, so that Wireless Stations can use either method ("Open System" or "Shared Key".). If you wish to use a particular method, select the appropriate value - "Open System" or "Shared Key". All Wireless stations must then be set to use the same method.
Data Encryption	Select the desired option, and ensure your Wireless stations have the same setting: • **64 Bit (10 Hex char)** - Keys are 10 Hex (5 ASCII) characters. • **128 Bit (26 Hex char)** - Keys are 26 Hex (13 ASCII) characters.
Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a **Key Value** for the **Default Key**.
Key Value	Enter the key value or values you wish to use. The **Key** is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

Security Settings - WPA-PSK

Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.

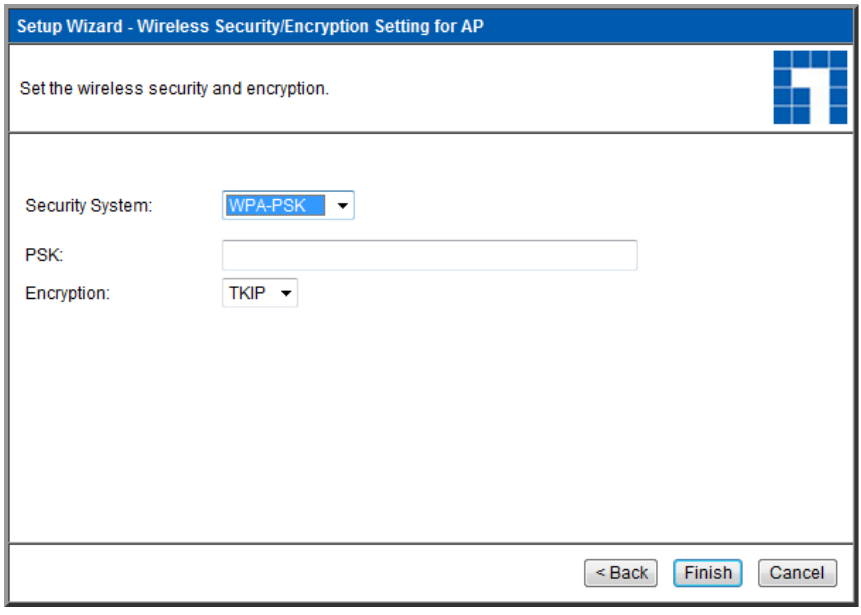


Figure 18: WPA-PSK Wireless Security Screen

Data - WPA-PSK Screen

WPA-PSK	
PSK	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
Encryption	The WPA-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.

Security Settings - WPA2-PSK

This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.

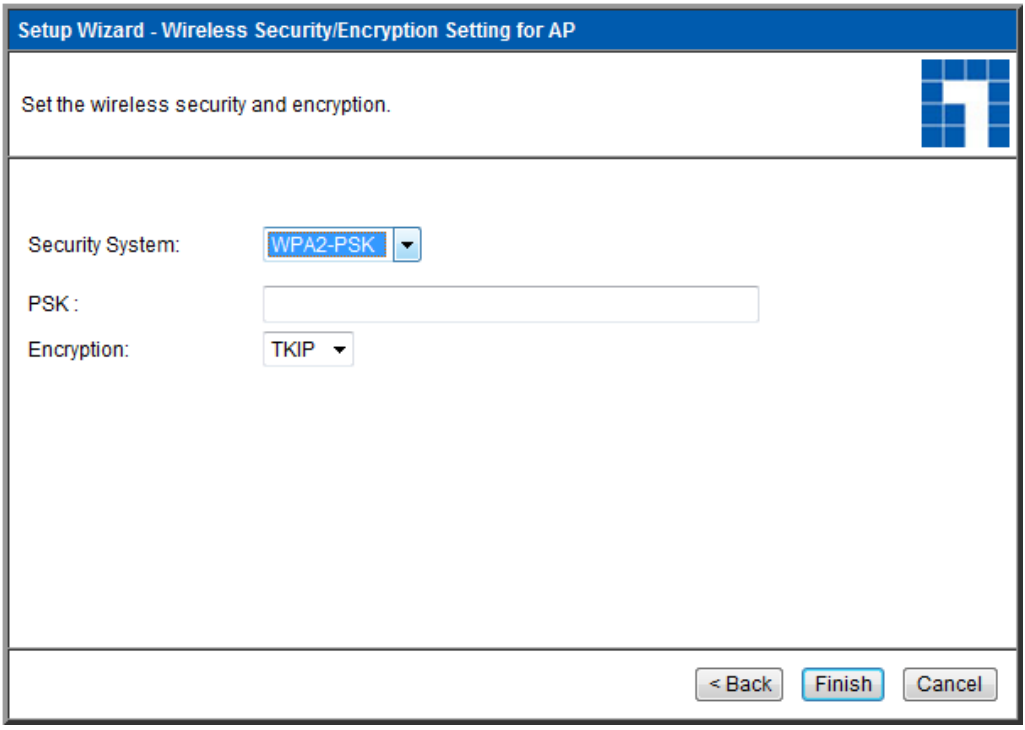


Figure 19: WPA2-PSK Wireless Security Screen

Data - WPA2-PSK Screen

WPA2-PSK	
PSK	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
Encryption	The WPA2-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.

Security Settings - 802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If this option is selected:

- This Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server. Normally, a Certificate is used to authenticate each user. See Chapter4 for details of user configuration.
- Each user's wireless client must support 802.1x.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

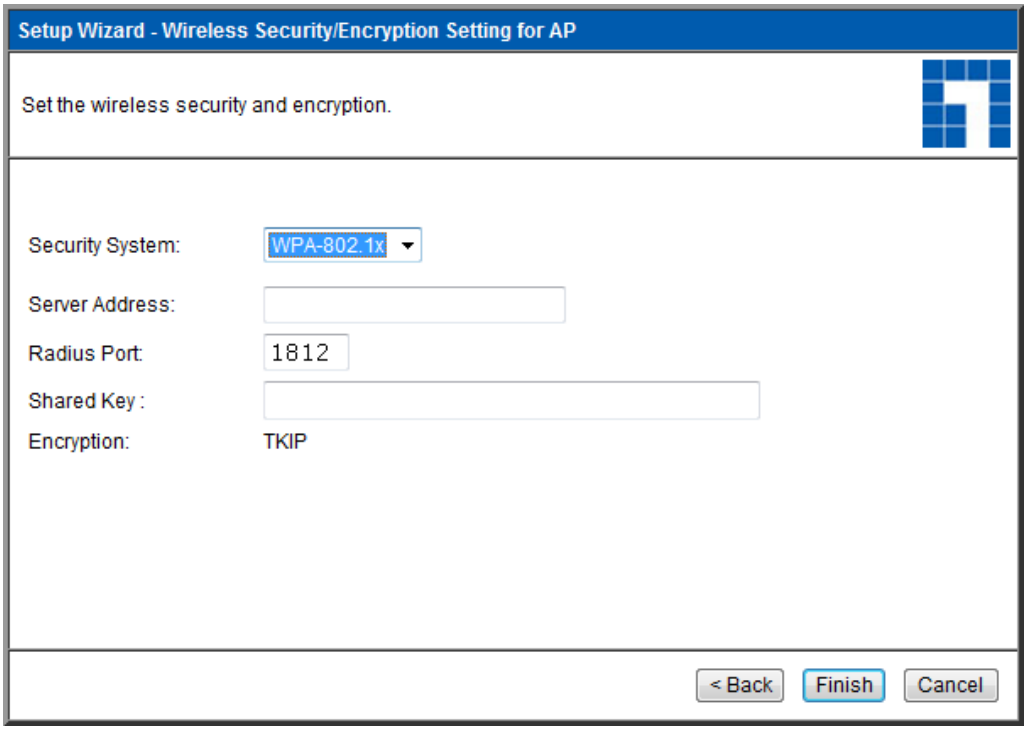


Figure 20: 802.1x Wireless Security Screen

Data - 802.1x Screen

Server Address	Enter the server address here.
Radius Port	Enter the port number used for connections to the Radius Server.
Shared Key	Enter the shared key. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same key. The key must be from 8 to 63 characters in length.
Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.

MAC Filter

Use this feature to determine which Wireless stations can use the Access Point.

Click *MAC Filter* on the main menu to view a screen like the following.

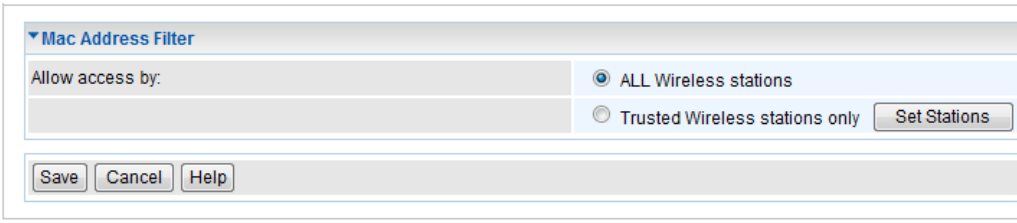


Figure 21: MAC Filter Screen

Data - MAC Filter Screen

MAC Filter	
Allow access by …	Use this feature to determine which Wireless stations can use the Access Point. The options are: • **All Wireless Stations** - All wireless stations can use the access point, provided they have the correct SSID and security settings. • **Trusted Wireless stations only** - Only wireless stations you designate as "Trusted" can use the Access Point, even if they have the correct SSID and security settings. This feature uses the MAC address to identify Wireless stations. The MAC address is a low-level network identifier which is unique to each PC or network device. To define the trusted wireless stations, use the "Set Stations" button.
Set Stations Button	Click this button to manage the trusted PC database.

Trusted Wireless Stations

To change the list of trusted wireless stations, use the *Modify List* button on the *Access Control* screen. You will see a screen like the sample below.

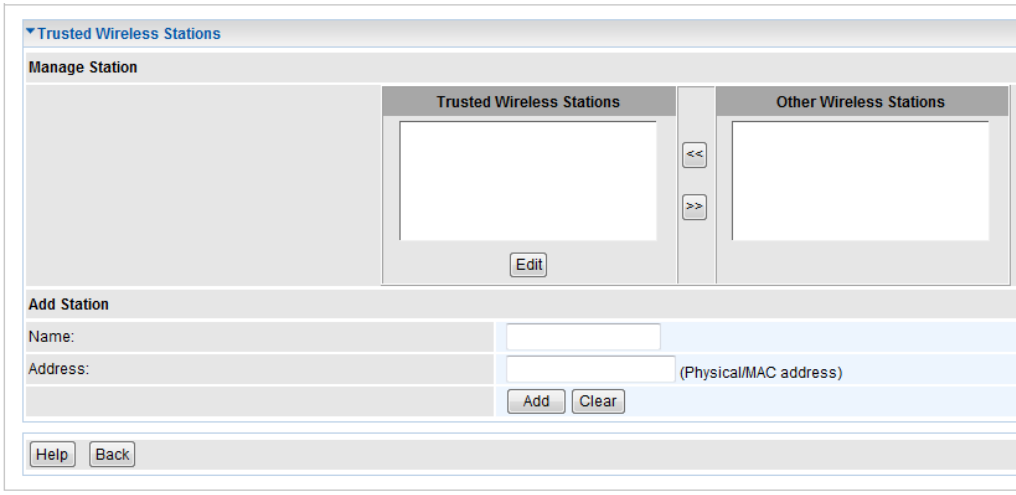


Figure 22: Trusted Wireless Stations

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as "Trusted".
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Buttons	
<<	Add a Trusted Wireless Station to the list (move from the "Other Stations" list). • Select an entry (or entries) in the "Other Stations" list, and click the " << " button. • Enter the Address (MAC or physical address) of the wireless station, and click the "Add " button.
>>	Delete a Trusted Wireless Station from the list (move to the "Other Stations" list). • Select an entry (or entries) in the "Trusted Stations" list. • Click the " >> " button.

Edit	To change an existing entry in the "Trusted Stations" list, select it and click this button. 1. Select the Station in the "Trusted Station" list. 2. Click the "Edit" button. The address will be copied to the "Address" field, and the "Add" button will change to "Update". 3. Edit the address (MAC or physical address) as required. 4. Click "Update" to save your changes.
Add	To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button.
Clear	Clear the *Name* and *Address* fields.

Wi-Fi Protected Setup

Click *WiFi Protected Setup* on the main menu to view a screen like the following:

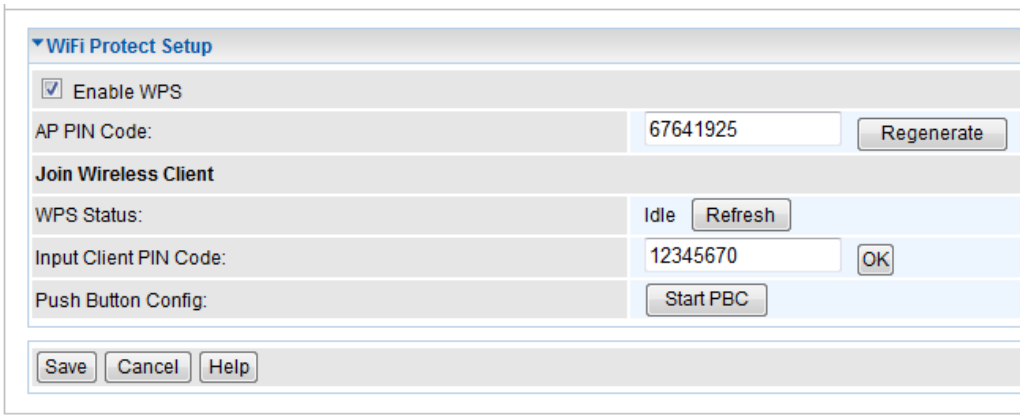


Figure 23: WPS Screen

Data - WPS Screen

WPS	
Enable WPS	WPS (Wi-Fi Protected Setup) was created and developed by the Wi-Fi Alliance. This feature can help to simplify the procedure of configuring security on a wireless network instead of entering all the required data manually. WPS only works with either WPA-PSK or WPA2-PSK encryption method.
AP PIN Code	Enter the desired pin value manually or click the G*enerate* button to have the new pin code displayed in the field.
Input Client PIN Code	Enter the PIN code from the client device in this field and click *OK* button.
Push Button Config	Push a simulated push button in the software on the wireless client to initiate WPS mode. You will also need to press the actual WPS button of the Wireless access Point. Click the *Start PBC* button.

Chapter 4
PC and Server Configuration

This Chapter details the PC Configuration required for each PC on the local LAN.

Overview

All Wireless Stations need to have settings which match the Wireless Access Point. These settings depend on the mode in which the Access Point is being used.

- If using WEP or WPA-PSK, it is only necessary to ensure that each Wireless station's settings match those of the Wireless Access Point, as described below.
- For 802.1x modes, configuration is much more complex. The Radius Server must be configured correctly, and setup of each Wireless station is also more complex.

Using WEP

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

Mode	On each PC, the mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Access Point. The default value is **`wireless`** **Note! The SSID is case sensitive.**
Wireless Security	• Each Wireless station must be set to use WEP data encryption. • The Key size (64 bit, 128 bit, 152 bit) must be set to match the Access Point. • The keys values on the PC must match the key values on the Access Point. **Note**: On some systems, the key sizes may be shown as 40bit, 104bit, and 128bit instead of 64 bit, 128 bit and 152bit. This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Using WPA-PSK/WPA2-PSK

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

Mode	On each PC, the mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Access Point. The default value is **`wireless`** **Note! The SSID is case sensitive.**
Wireless Security	On each client, Wireless security must be set to WPA-PSK. • The **Pre-shared Key** entered on the Access Point must also be entered on each Wireless client. • The **Encryption** method (e.g. TKIP, AES) must be set to match the Access Point.

802.1x Server Setup (Windows 2000 Server)

This section describes using *Microsoft Internet Authentication Server* as the Radius Server, since it is the most common Radius Server available that supports the EAP-TLS authentication method.

The following services on the Windows 2000 Domain Controller (PDC) are also required:

- dhcpd
- dns
- rras
- webserver (IIS)
- Radius Server (Internet Authentication Service)
- Certificate Authority

Windows 2000 Domain Controller Setup

1. Run *dcpromo.exe* from the command prompt.
2. Follow all of the default prompts, ensure that DNS is installed and enabled during installation.

Services Installation

1. Select the *Control Panel - Add/Remove Programs*.
2. Click *Add/Remove Windows Components* from the left side.
3. Ensure that the following components are activated (selected):
   - *Certificate Services*. After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select *Yes* to select certificate services and continue
   - *World Wide Web Server*. Select *World Wide Web Server* on the *Internet Information Services* (IIS) component.
   - From the *Networking Services* category, select *Dynamic Host Configuration Protocol* (DHCP), and *Internet Authentication Service* (DNS should already be selected and installed).

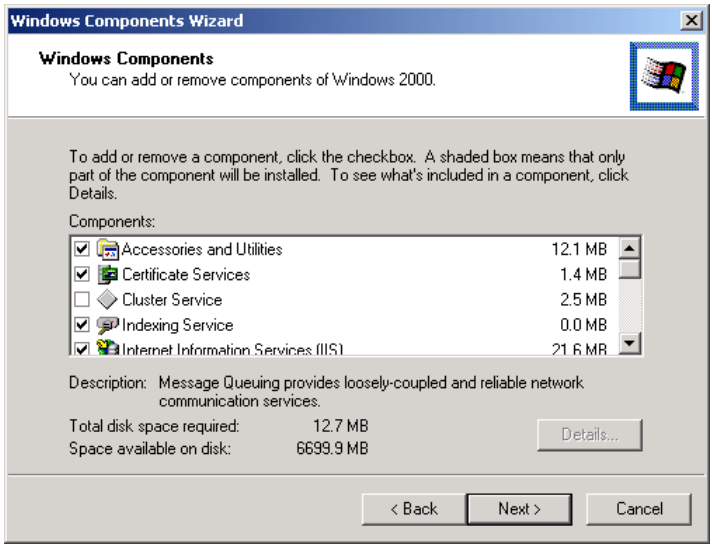

Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 12.1 MB
Certificate Services 1.4 MB
Cluster Service 2.5 MB
Indexing Service 0.0 MB
Internet Information Services (IIS) 21.6 MB
Description: Message Queuing provides loosely-coupled and reliable network communication services.
Total disk space required: 12.7 MB
Space available on disk: 6699.9 MB
Details...
< Back
Next >
Cancel

Figure 24: Components Screen

4. Click *Next*.
5. Select the *Enterprise root CA*, and click *Next*.

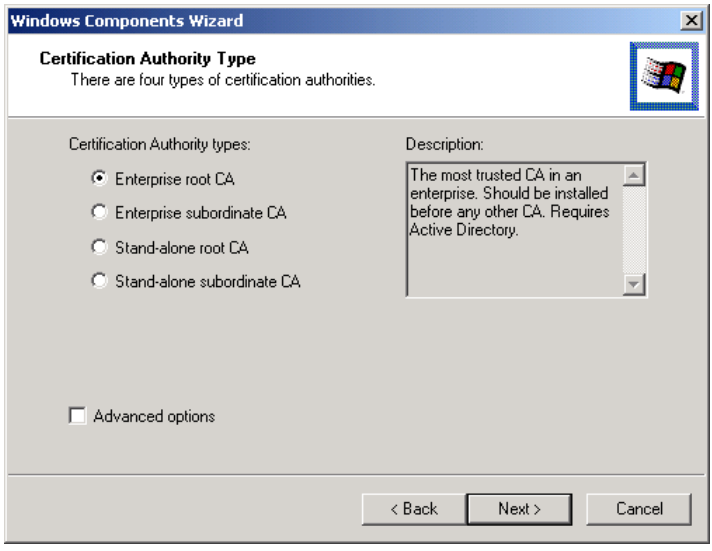

Windows Components Wizard
Certification Authority Type
There are four types of certification authorities.
Certification Authority types:
Enterprise root CA
Enterprise subordinate CA
Stand-alone root CA
Stand-alone subordinate CA
Description:
The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.
Advanced options
< Back
Next >
Cancel

Figure 25: Certification Screen

6. Enter the information for the Certificate Authority, and click *Next*.

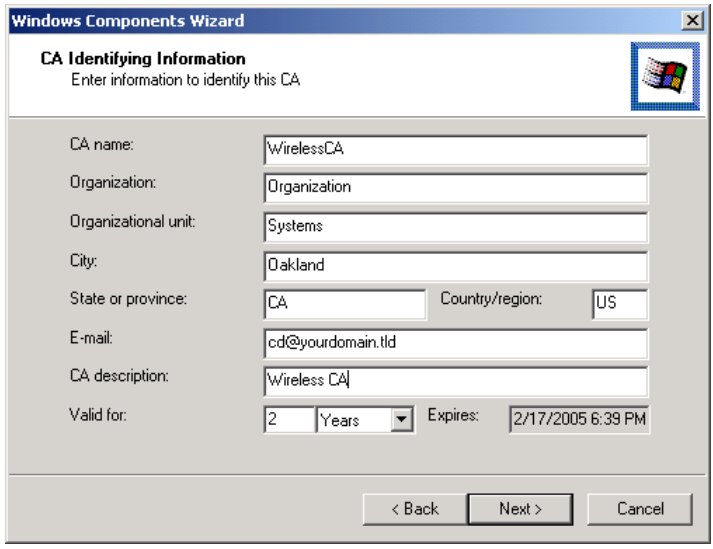


Figure 26: CA Screen

7. Click *Next* if you don't want to change the CA's configuration data.
8. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click *Ok*, then *Finish*.

DHCP server configuration

1. Click on the *Start - Programs - Administrative Tools - DHCP*
2. Right-click on the server entry as shown, and select *New Scope*.

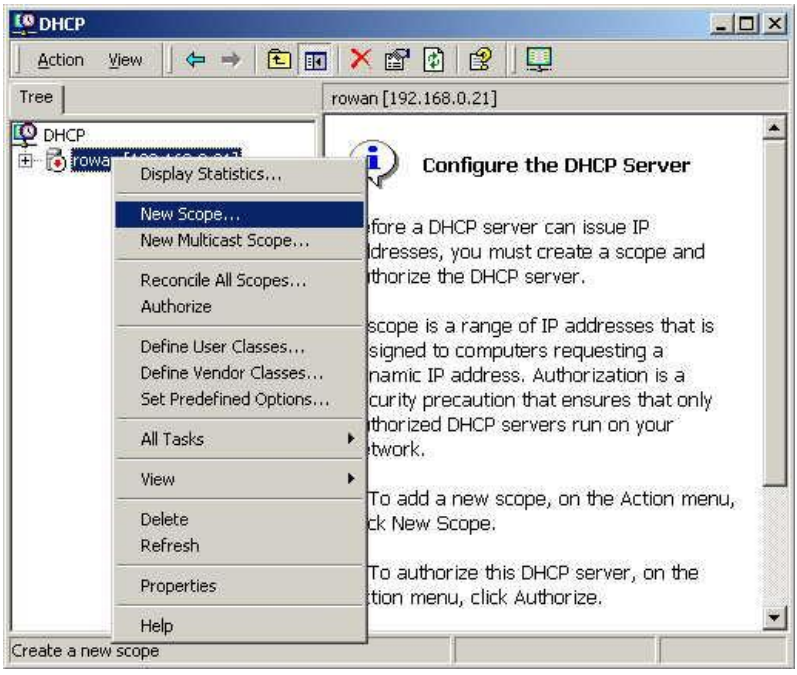


Figure 27: DHCP Screen

3. Click *Next* when the New Scope Wizard Begins.
4. Enter the name and description for the scope, click *Next*.
5. Define the IP address range. Change the subnet mask if necessary. Click *Next*.

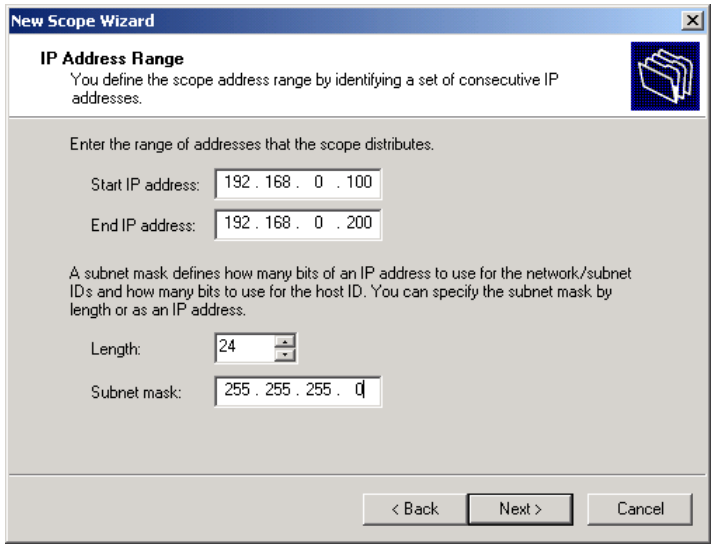

New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address:
192 . 168 . 0 . 100
End IP address:
192 . 168 . 0 . 200
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.
Length:
24
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel

Figure 28:IP Address Screen

6. Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click *Next*.
7. Change the *Lease Duration* time if preferred. Click *Next*.
8. Select *Yes, I want to configure these options now*, and click *Next*.
9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click *Next*.
10. For the Parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address. Click *Next*.

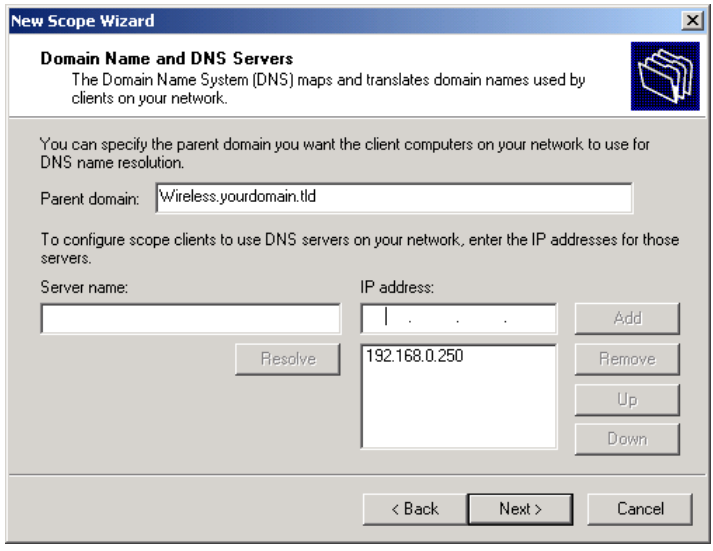

New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
Wireless.yourdomain.tld
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
192.168.0.250
Remove
Up
Down
< Back
Next >
Cancel

Figure 29: DNS Screen

11. If you don't want a WINS server, just click *Next*.
12. Select *Yes, I want to activate this scope now*. Click *Next*, then *Finish*.
13. Right-click on the server, and select *Authorize*. It may take a few minutes to complete.

Certificate Authority Setup

1. Select *Start - Programs - Administrative Tools - Certification Authority*.
2. Right-click *Policy Settings*, and select *New - Certificate to Issue*.

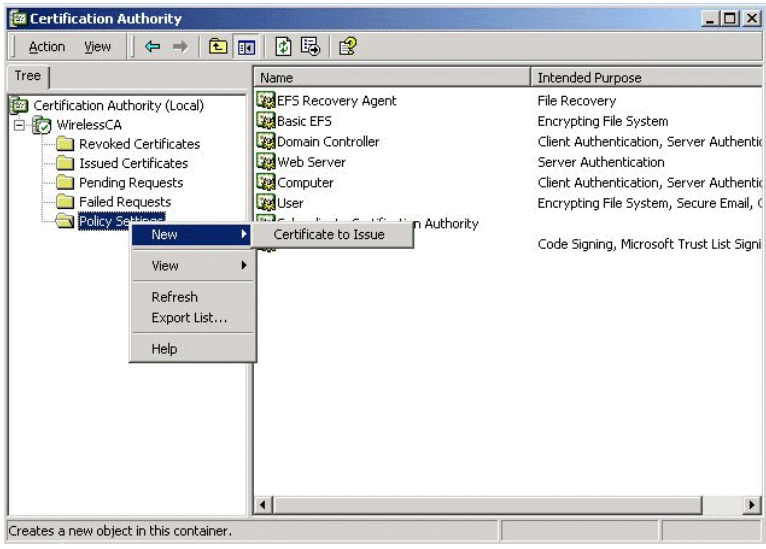


Figure 30: Certificate Authority Screen

3. Select *Authenticated Session* and *Smartcard Logon* (select more than one by holding down the Ctrl key). Click *OK*.

Figure 31: Template Screen

4. Select *Start - Programs - Administrative Tools - Active Directory Users and Computers.*
5. Right-click on your active directory domain, and select *Properties.*

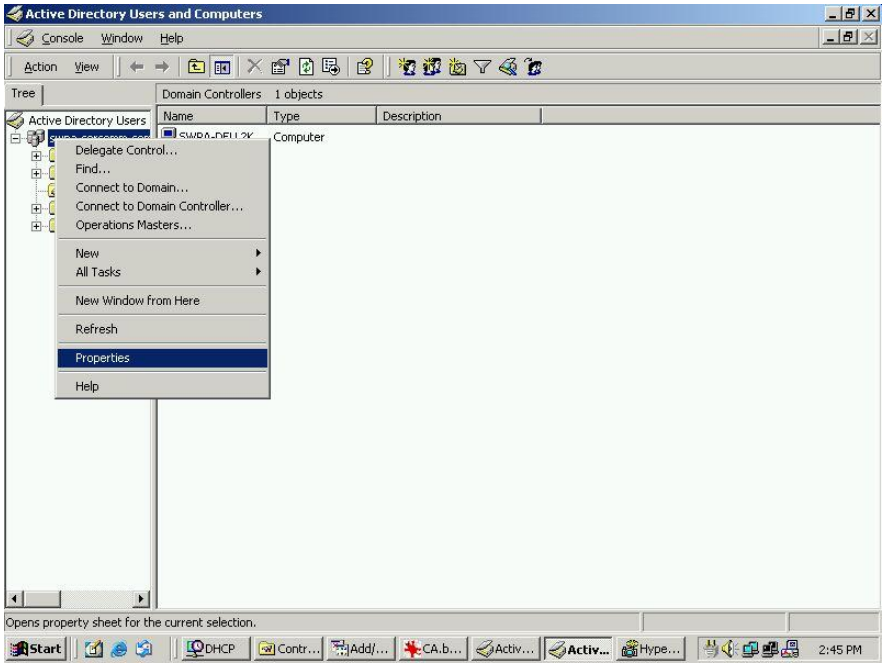


Figure 32: Active Directory Screen

6. Select the *Group Policy* tab, choose *Default Domain Policy* then click *Edit*.

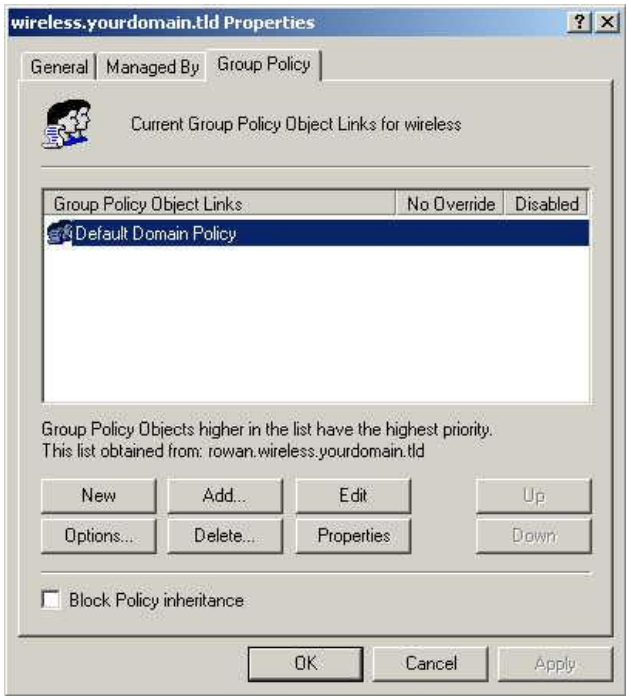


Figure 33: Group Policy Tab

7. Select *Computer Configuration - Windows Settings - Security Settings - Public Key Policies*, right-click *Automatic Certificate Request Settings - New - Automatic Certificate Request*.

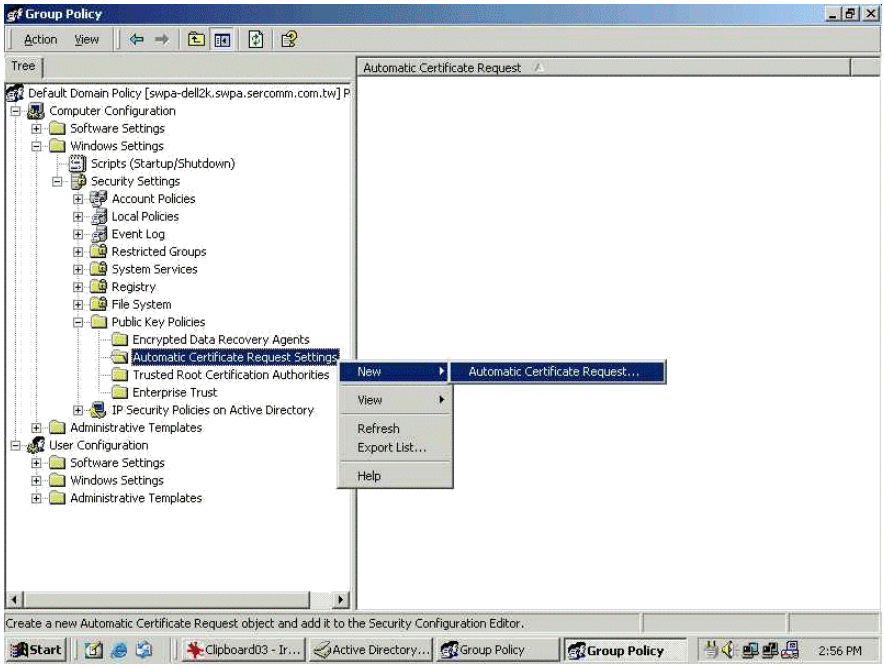


Figure 34: Group Policy Screen

8. When the Certificate Request Wizard appears, click *Next*.
9. Select *Computer*, then click *Next*.

Automatic Certificate Request Setup Wizard
Certificate Template
The next time a computer logs on, a certificate based on the template you select is provided.
A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.
Certificate templates:
Name
Intended Purposes
Computer
Client Authentication, Server Authentication
Domain Controller
Client Authentication, Server Authentication
Enrollment Agent (Computer)
Certificate Request Agent
IPSEC
1.3.6.1.5.5.8.2.2
< Back
Next >
Cancel

Figure 35: Certificate Template Screen

10. Ensure that your certificate authority is checked, then click *Next*.
11. Review the policy change information and click *Finish*.
12. Click *Start* - *Run*, type *cmd* and press enter.
    Enter `secedit /refreshpolicy machine_policy`
    This command may take a few minutes to take effect.

Internet Authentication Service (Radius) Setup

1. Select *Start - Programs - Administrative Tools - Internet Authentication Service*
2. Right-click on *Clients*, and select *New Client*.

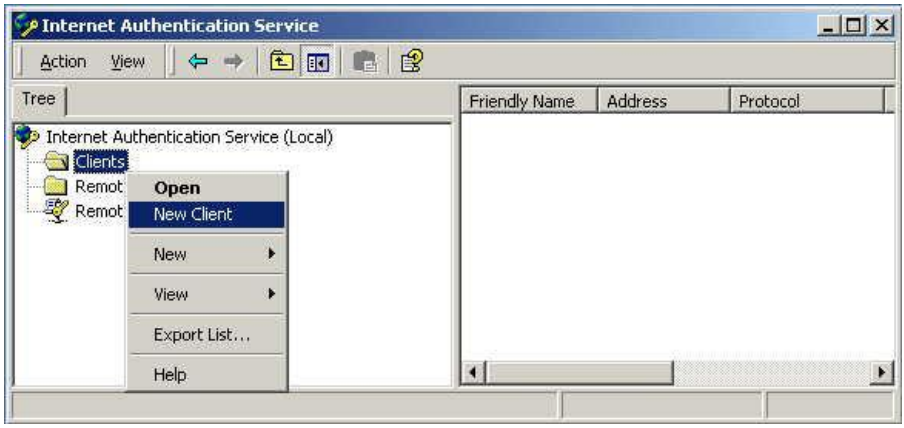


Figure 36: Service Screen

3. Enter a name for the access point, click *Next*.
4. Enter the address or name of the Wireless Access Point, and set the shared secret, as entered on the *Security Settings* of the Wireless Access Point.
5. Click *Finish*.
6. Right-click on *Remote Access Policies*, select *New Remote Access Policy*.
7. Assuming you are using EAP-TLS, name the policy `eap-tls`, and click *Next*.
8. Click *Add...*
   If you don't want to set any restrictions and a condition is required, select *Day-And-Time-Restrictions*, and click *Add...*

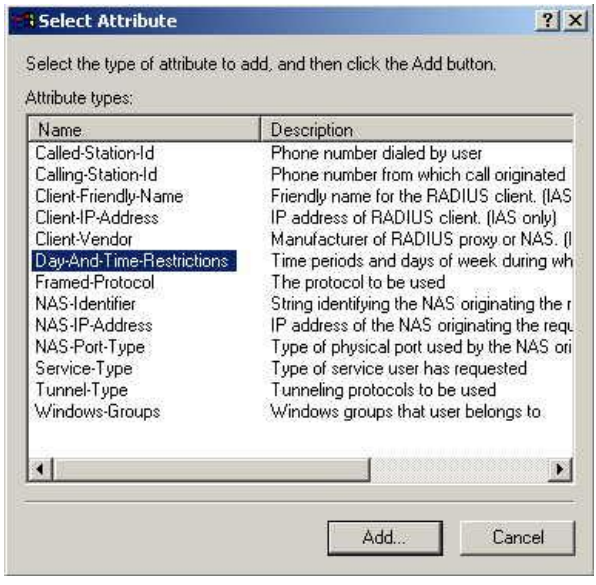


Figure 37: Attribute Screen

9. Click *Permitted*, then *OK*. Select *Next*.
10. Select *Grant remote access permission*. Click *Next*.

11. Click *Edit Profile...* and select the *Authentication* tab. Enable *Extensible Authentication Protocol*, and select *Smart Card or other Certificate*. Deselect other authentication methods listed. Click *OK*.

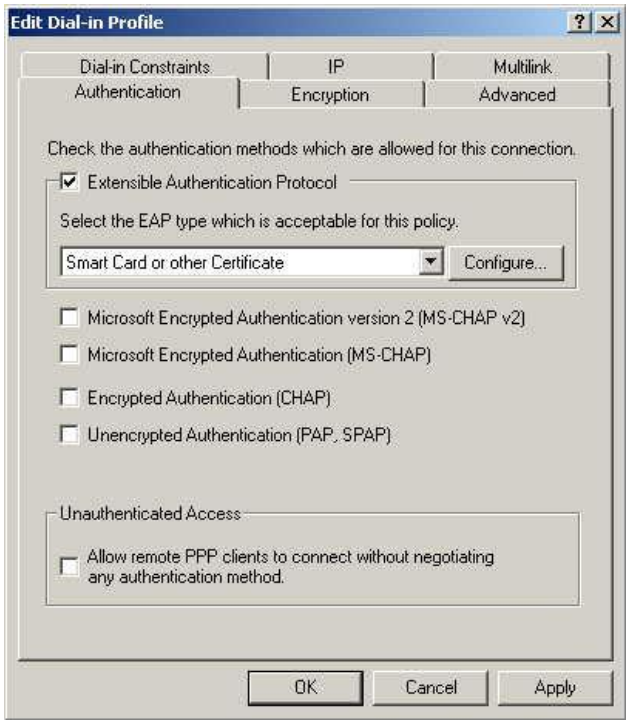


Figure 38: Authentication Screen

12. Select *No* if you don't want to view the help for EAP. Click *Finish*.

Remote Access Login for Users

1. Select *Start - Programs - Administrative Tools- Active Directory Users and Computers*.
2. Double click on the user who you want to enable.
3. Select the *Dial-in* tab, and enable *Allow access*. Click *OK*.

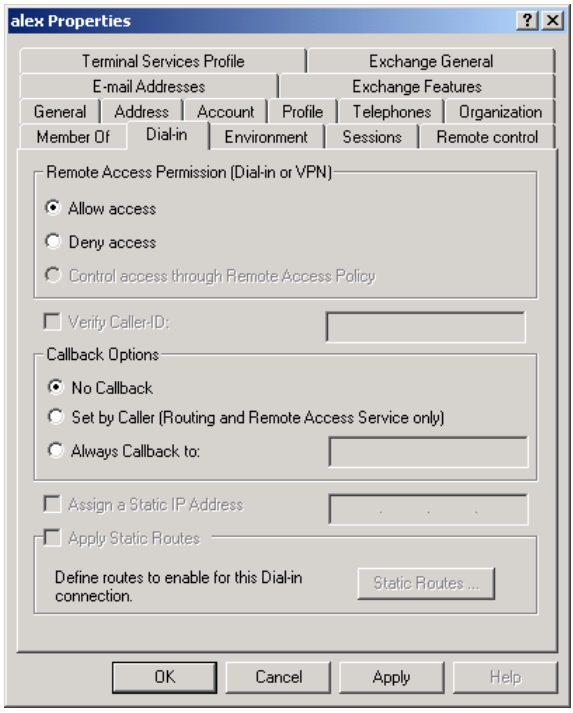


Figure 39: Dial-in Screen

802.1x Client Setup on Windows XP

Windows XP ships with a complete 802.1x client implementation. If using Windows 2000, you can install SP3 (Service Pack 3) to gain the same functionality.

If you don't have either of these systems, you must use the 802.1x client software provided with your wireless adapter. Refer to your vendor's documentation for setup instructions.

The following instructions assume that:

- You are using Windows XP
- You are connecting to a Windows 2000 server for authentication.
- You already have a login (User name and password) on the Windows 2000 server.

Client Certificate Setup

1. Connect to a network which doesn't require port authentication.
2. Start your Web Browser. In the *Address* box, enter the IP address of the Windows 2000 Server, followed by */certsrv*
   e.g
   `http://192.168.0.2/certsrv`
3. You will be prompted for a user name and password. Enter the *User name* and *Password* assigned to you by your network administrator, and click *OK*.

Figure 40: Connect Screen

4. On the first screen (below), select *Request a certificate*, click *Next*.

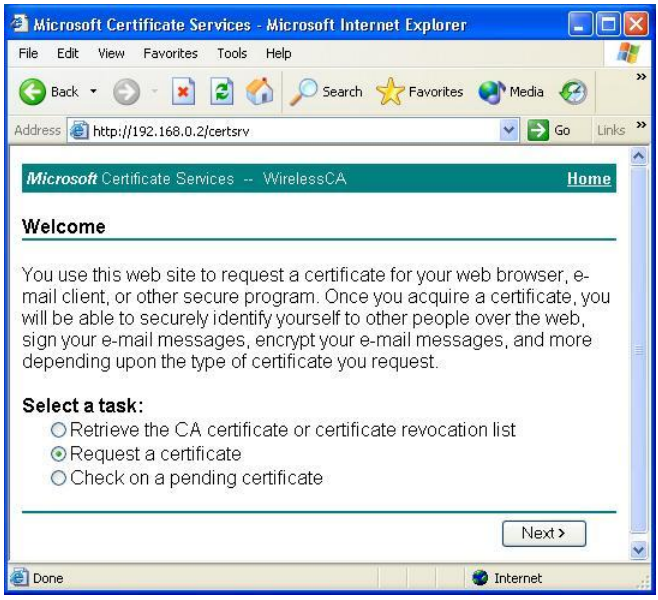

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.2/certsrv
Go Links
Microsoft Certificate Services -- WirelessCA
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >
Done
Internet

Figure 41: Wireless CA Screen

5. Select *User certificate request* and select *User Certificate*, the click *Next*.

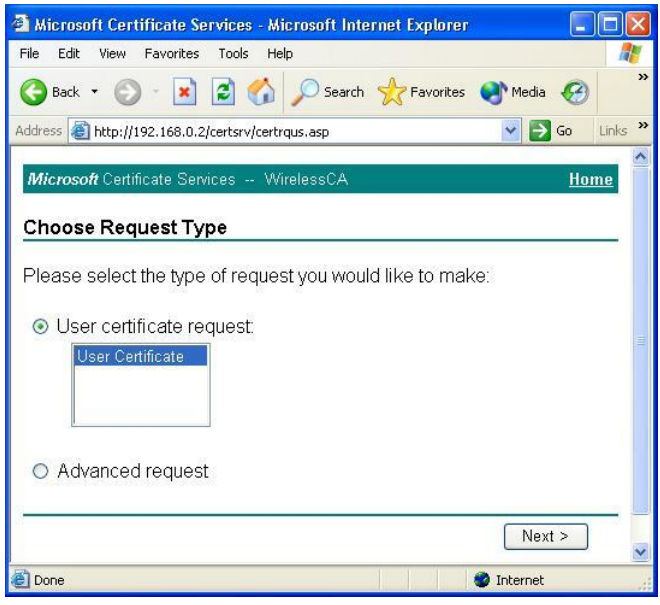


Figure 42: Request Type Screen

6. Click *Submit*.

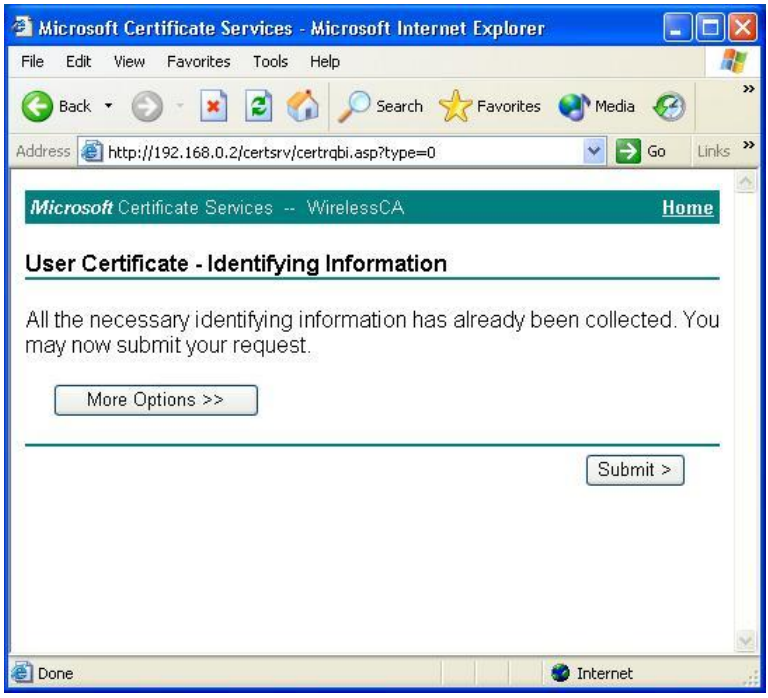

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.2/certsrv/certrqbi.asp?type=0
Go Links
Microsoft Certificate Services -- WirelessCA
Home
User Certificate - Identifying Information
All the necessary identifying information has already been collected. You may now submit your request.
More Options >>
Submit >
Done
Internet

Figure 43: Identifying Information Screen

7. A message will be displayed, then the certificate will be returned to you. Click *Install this certificate*.

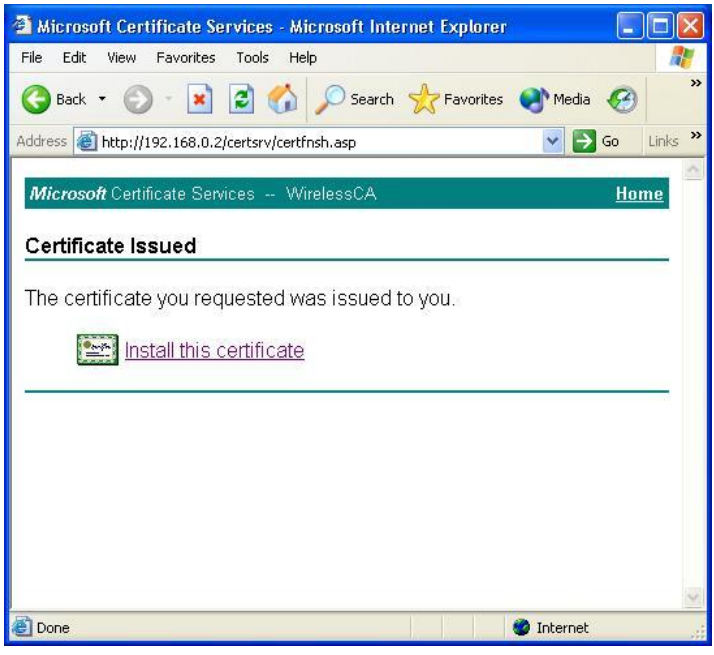


Figure 44:Certificate Issued Screen

8. . You will receive a confirmation message. Click *Yes*.

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : WirelessCA, Systems, Wireless Widgets, College Park, MD, US, ca@yourdomain.tld
Issuer : Self Issued
Time Validity : Thursday, October 11, 2001 through Saturday, October 11, 2003
Serial Number : 76E7A8D0 B63756A3 4F77E081 551337C7
Thumbprint (sha1) : E9EC3F5D BA9B678E 79C055A8 51017043 BE7A0CB7
Thumbprint (md5) : 6F171E64 D438B251 A4242464 CD8E6189
Yes
No

Figure 45: Root Certificate Screen

9. Certificate setup is now complete.

802.1x Authentication Setup

1. Open the properties for the wireless connection, by selecting *Start - Control Panel - Network Connections.*
2. Right Click on the *Wireless Network Connection*, and select *Properties*.
3. Select the *Authentication* Tab, and ensure that *Enable network access control using IEEE 802.1X* is selected, and *Smart Card or other Certificate* is selected from the EAP type.

Wireless Network Connection Properties
General
Wireless Networks
Authentication
Advanced
Select this option to provide authenticated network access for wired and wireless Ethernet networks.
Enable network access control using IEEE 802.1X
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

Figure 46: Authentication Tab

Encryption Settings

The Encryption settings must match the APs (Access Points) on the Wireless network you wish to join.

- Windows XP will detect any available Wireless networks, and allow you to configure each network independently.

- Your network administrator can advise you of the correct settings for each network. 802.1x networks typically use EAP-TLS. This is a dynamic key system, so there is no need to enter key values.

Enabling Encryption

To enable encryption for a wireless network, follow this procedure:

1. Click on the *Wireless Networks* tab.

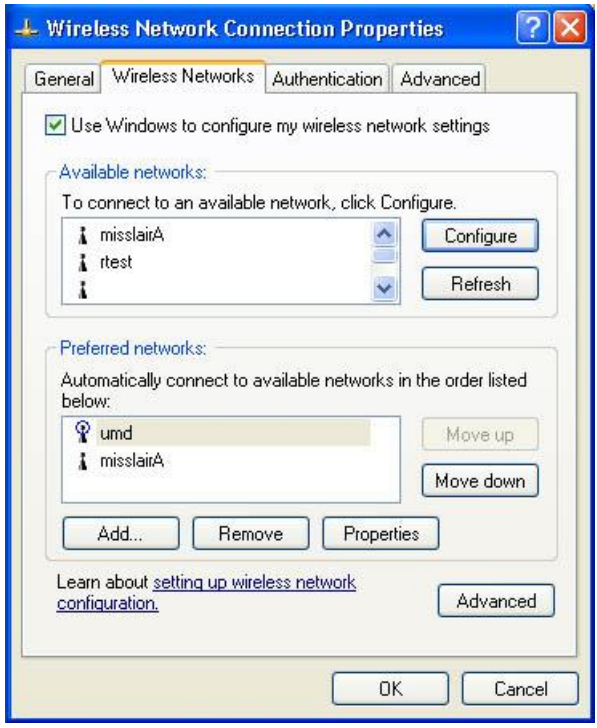


Figure 47: Wireless Networks Screen

2. Select the wireless network from the *Available Networks* list, and click *Configure*.
3. Select and enter the correct values, as advised by your Network Administrator.
   For example, to use EAP-TLS, you would enable *Data encryption*, and click the checkbox for the setting *The key is provided for me automatically*, as shown below.

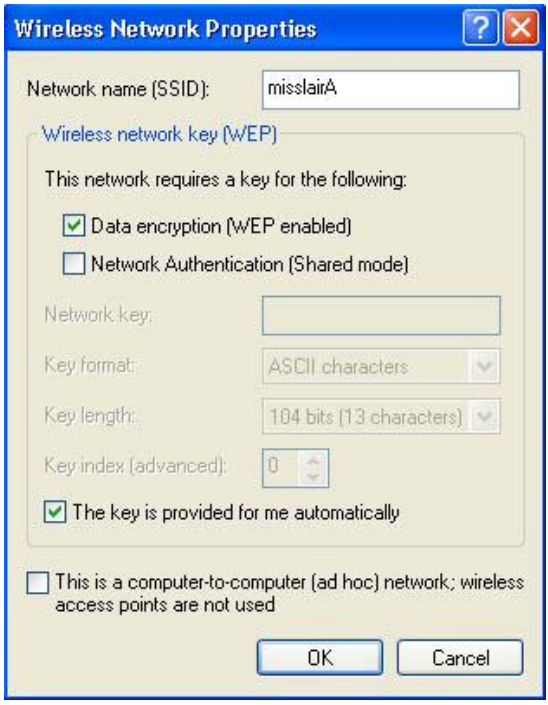


Figure 48: Properties Screen

Setup for Windows XP and 802.1x client is now complete.

Using 802.1x Mode (without WPA)

This is very similar to using WPA-Enterprise.

The only difference is that on your client, you must NOT enable the setting *The key is provided for me automatically*.

Instead, you must enter the WEP key manually, ensuring it matches the WEP key used on the Access Point.

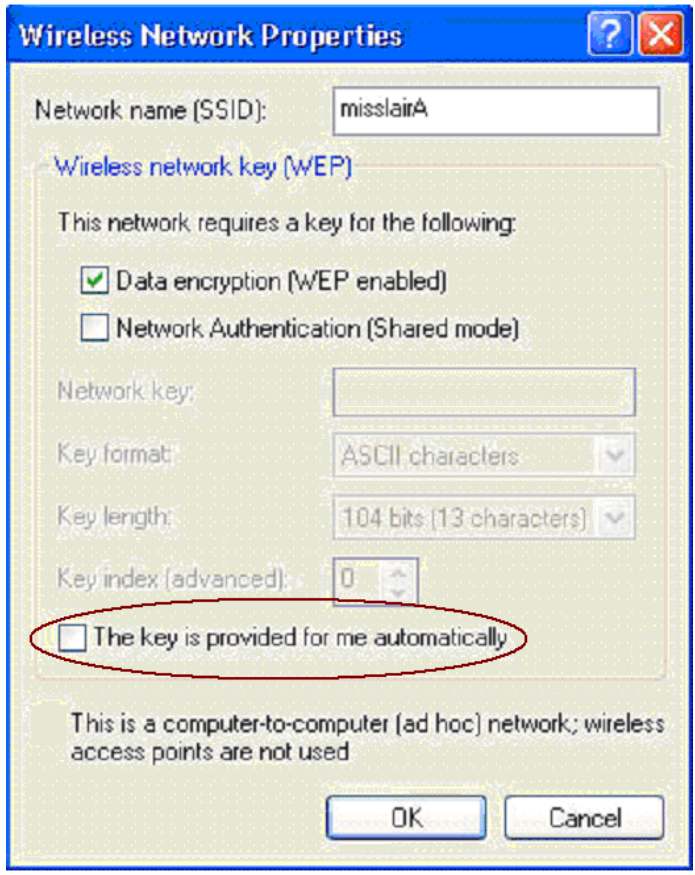


Figure 49: Properties Screen

Note:

On some systems, the "64 bit" WEP key is shown as "40 bit" and the "128 bit" WEP key is shown as "104 bit". This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Chapter 5
Access Point Management

This Chapter explains when and how to use the Wireless Access Point's "Management" Features.

Overview

This Chapter covers the following features, available on the Wireless Access Point's ***Management*** menu.

- Status
- Password
- Config File
- Upgrade Firmware

Status Screen

Use the ***Status*** link on the main menu to view this screen.

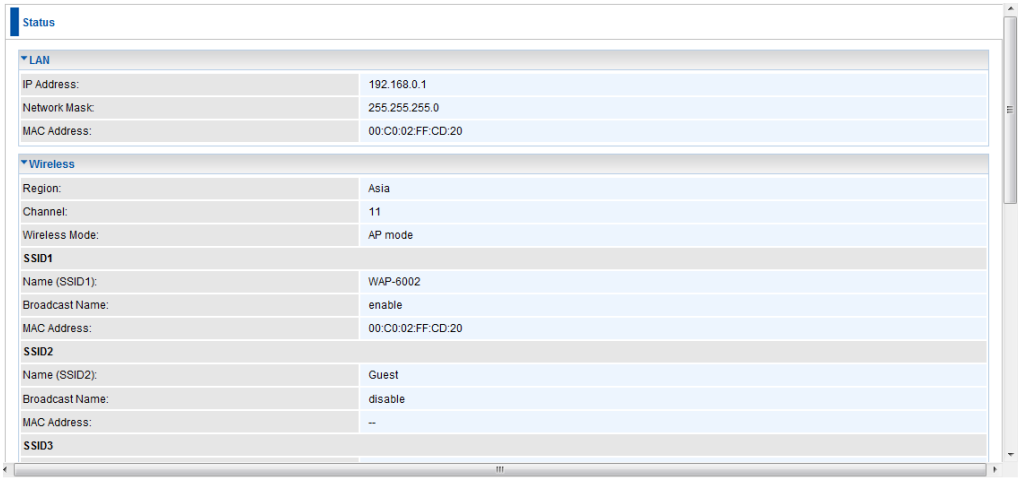


Figure 50: Status Screen

Data - Status Screen

Ether	
IP Address	The IP Address of the Wireless Access Point.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
MAC Address	The MAC (physical) address of the Wireless Access Point.
Wireless	
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Name (SSID 1/2)	It displays the name of the SSID 1/2.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
MAC Address	The MAC (physical) address of the Wireless Access Point.
System	
Device Name	The current name of the Wireless Access Point. This name is also the "hostname" for users with an "@Home" type connection.
Firmware Version	The version of the current firmware installed.
Current Time	It displays the current time of the system.
Buttons	
Refresh Screen	Update the data displayed on screen.

Password Screen

The *Password* screen allows you to assign a password to the Wireless Access Point. This password limits access to the configuration interface. The default password is *password*. It is recommended that this be changed, using this screen.

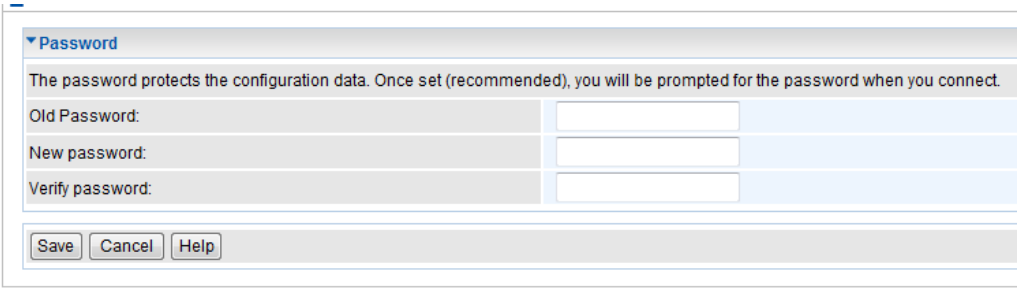


Figure 51: Password Screen

Data - Password Screen

Login	
Old Password	If you wish to change the Admin password, check this field and enter the new login password in the fields below.
New Password	Enter the desired login password.
Verify Password	Re-enter the desired login password.

Config File

This screen allows you to Backup (download) the configuration file, and to restore (upload) a previously-saved configuration file.

You can also set the Wireless Access Point back to its factory default settings.

To reach this screen, select *Config File* in the main menu.

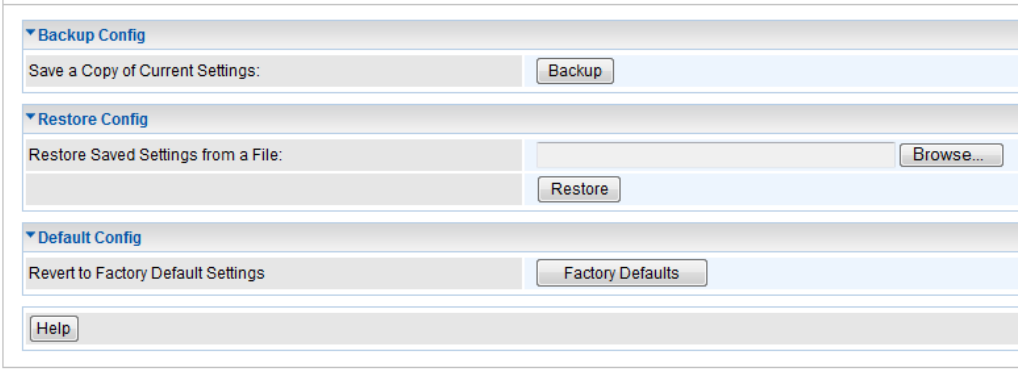


Figure 52: Config File Screen

Data - Config File Screen

Backup	
Save a copy of current settings	Once you have the Access Point working properly, you should back up the settings to a file on your computer. You can later restore the Access Point's settings from this file, if necessary. To create a backup file of the current settings: • Click **Backup**. • If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click **Save**.
Restore	
Restore saved settings from a file	To restore settings from a backup file: 1. Click **Browse**. 2. Locate and select the previously saved backup file. 3. Click **Restore**
Defaults	
Revert to factory default settings	To erase the current settings and restore the original factory default settings, click **Factory Defaults** button. **Note!** • This will terminate the current connection. The Access Point will be unavailable until it has restarted. • By default, the Access Point will act as a DHCP client, and automatically obtain an IP address. You will need to determine its new IP address in order to re-connect.

Firmware Upgrade

The firmware (software) in the Wireless Access Point can be upgraded using your Web Browser.

You must first download the upgrade file, and then select *Upgrade Firmware* in the main menu. You will see a screen like the following.

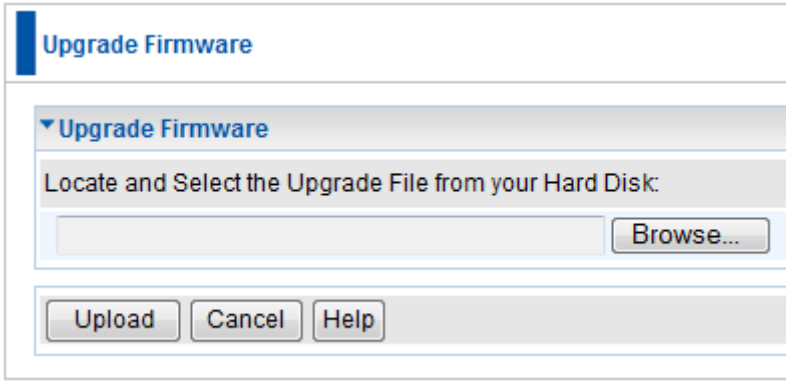


Figure 53: Firmware Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the *Upload* button to commence the firmware upgrade.

The Wireless Access Point is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless Access Point will be lost.

Appendix A
Specifications

Wireless Access Point

Hardware Specifications

SDRAM	16 Mbytes
Flash ROM	4 Mbytes
LAN port	1 x Auto-MDIX RJ 45 for 10/100Mbps Ethernet
Operating temperature	0° C to 40° C
Storage temperature	-20° C to 70° C
Power Adapter	12VDC 1A External
Dimensions	125mm(W) * 123mm(D) * 31mm(H)

Wireless Specifications

Standard	Network Standard IEEE 802.11n 2.0, IEEE 802.11b and IEEE 802.11g compliance
Transfer Rate	IEEE802.11b 11M/5.5M/2M/1M
	IEEE802.11g 54M/48M/36M/24M/18M/12M/11M/9M/6M
	IEEE802.11n 2.0 300M/270M/243M/240M/216M/180M/162M/120M/108 Mbps in 40Mhz mode 145M/130M/117M/104M/78Mbps in 20Mhz mode
Bandwidth	IEEE802.11b: Over 5Mbps
	IEEE802.11g: Over 20Mbps
	IEEE802.11n 2.0: Over 60Mbps (20Mhz mode) /100 Mbps (40Mhz mode)
Channels	2.4GHz ~ 2.485GHz / 1~13 channels
Transmission mode	IEEE802.11b: CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
	IEEE802.11g: OFDM
	IEEE802.11n 2.0: OFDM
Transmit Range	Indoor 200~280m/outdoor 450~600m
Modulation	IEEE802.11b DBPSK / DQPSK / CCK

	IEEE802.11g BPSK / QPSK / 16-QAM/64-QAM/ OFDM
	IEEE802.11n 2.0 BPSK / QPSK / 16-QAM/64-QAM/ OFDM
Security	WEP (64/128), WPA/WPA-PSK (Personal), WPA2/WPA-PSK (Personal), TKIP, AES, Stealth AP (Hidden ESSID), MAC address filtering, WPS button support, Wireless client Isolation, 802.1x w/Radius
Antenna power	1.8dBi

Firmware Specifications

Feature	Details
Wireless	• Windows98SE/ME/2000(SP4)/XP SP2/Vista/7/MAC OSX/Linux
Recommended browser	• Microsoft Internet Explorer, Safari Ver1.2
Protocol Support	• NTP (Network Time Protocol)
Management	• Web based configuration • SNMP v1/v2c
Wireless Security	• WEP (64/128bit), WPA, WPA-PSK, and WPA2-PSK authentication • 802.1x w/Radius • MAC address filtering • TKIP • AES
Firmware Upgrade	• HTTP upgrade
Operation Mode	• AP Mode • AP Client Mode • Bridge Mode • WDS Mode • Repeater Mode

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B
Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless Access Point and some possible solutions to them. If you follow the suggested steps and the Wireless Access Point still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless Access Point to configure it.**

Solution 1: Check the following:

- The Wireless Access Point is properly installed, LAN connections are OK, and it is powered ON. Check the LEDs for port status.
- Ensure that your PC and the Wireless Access Point are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- You can use the following method to determine the IP address of the Wireless Access Point, and then try to connect using the IP address, instead of the name.

To Find the Access Point's IP Address

1. Open a MS-DOS Prompt or Command Prompt Window.
2. Use the Ping command to "ping" the Wireless Access Point. Enter `ping` followed by the Default Name of the Wireless Access Point. e.g.

   ```
   ping SC003318
   ```

3. Check the output of the ping command to determine the IP address of the Wireless Access Point, as shown below.

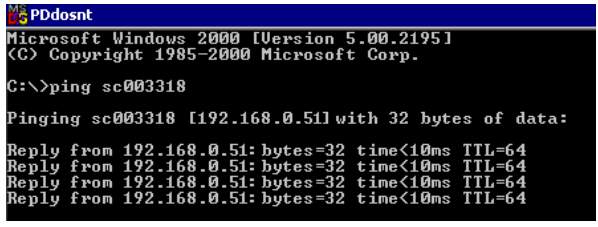

PDdosnt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ping sc003318
Pinging sc003318 [192.168.0.51] with 32 bytes of data:
Reply from 192.168.0.51: bytes=32 time<10ms TTL=64
Reply from 192.168.0.51: bytes=32 time<10ms TTL=64
Reply from 192.168.0.51: bytes=32 time<10ms TTL=64
Reply from 192.168.0.51: bytes=32 time<10ms TTL=64

Figure 54: Ping

If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address which is compatible with the Wireless Access Point. (If no DHCP Server is found, the Wireless Access Point will default to an IP Address and Mask of 192.168.0.1 and 255.255.255.0.) On Windows PCs, you can use *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Problem 2: **My PC can't connect to the LAN via the Wireless Access Point.**

Solution 2 Check the following:

- The SSID and WEP settings on the PC match the settings on the Wireless Access Point.
- On the PC, the wireless mode is set to "Infrastructure"
- If using the *Access Control* feature, the PC's name and address is in the *Trusted Stations* list.
- If using 802.1x mode, ensure the PC's 802.1x software is configured correctly. See Chapter 4 for details of setup for the Windows XP 802.1x client. If using a different client, refer to the vendor's documentation.

Appendix C
Windows TCP/IP

Overview

Normally, no changes need to be made.

- By default, the Wireless Access Point will act as a DHCP client, automatically obtaining a suitable IP Address (and related information) from your DHCP Server.
- If using Fixed (specified) IP addresses on your LAN (instead of a DHCP Server), there is no need to change the TCP/IP of each PC. Just configure the Wireless Access Point to match your existing LAN.

The following sections provide details about checking the TCP/IP settings for various types of Windows, should that be necessary.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

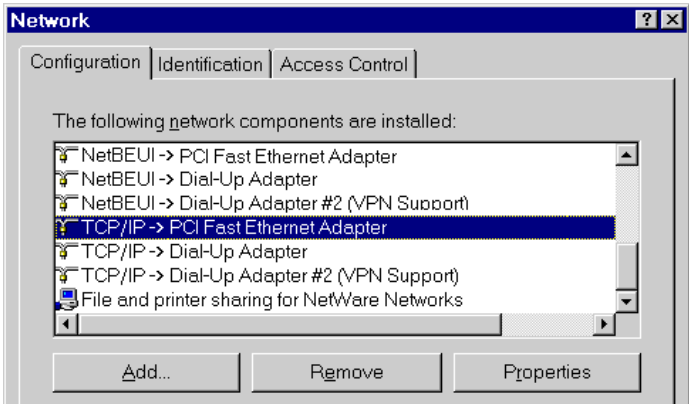


Figure 55: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

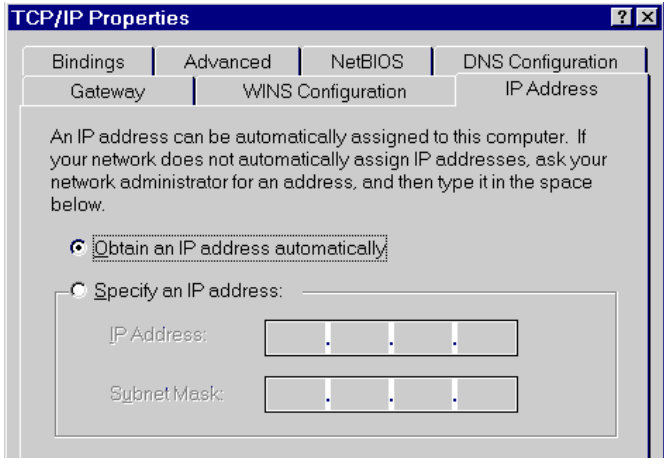

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

Figure 56: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings. To work correctly, you need a DHCP server on your LAN.

Using "Specify an IP Address"

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.

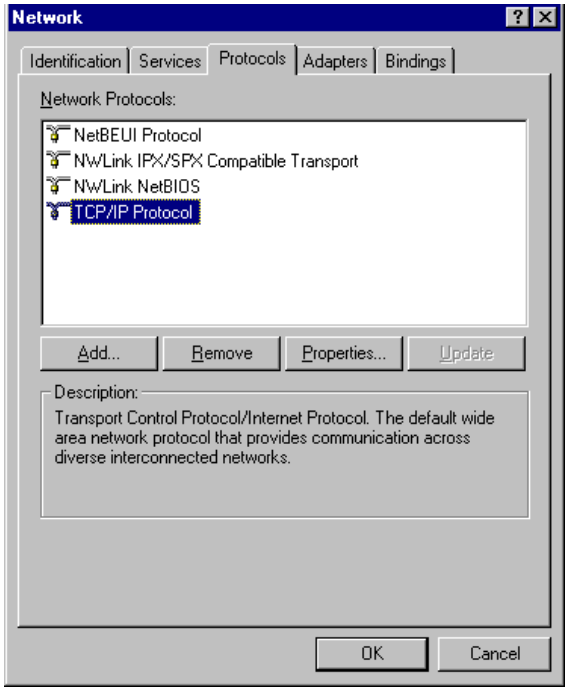


Figure 57: Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.

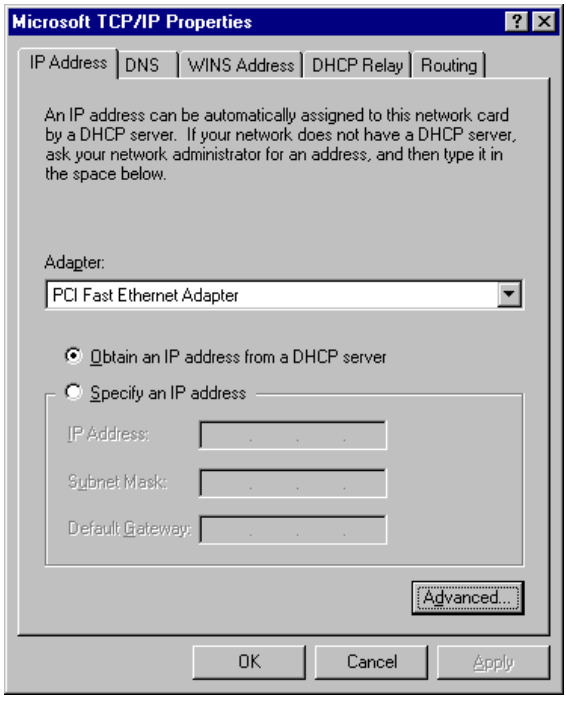

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
DHCP Relay
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
PCI Fast Ethernet Adapter
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Figure 58: Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

Obtain an IP address from a DHCP Server

This is the default Windows setting. This is the default Windows settings. To work correctly, you need a DHCP server on your LAN.

Using "Specify an IP Address"

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows 2000

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

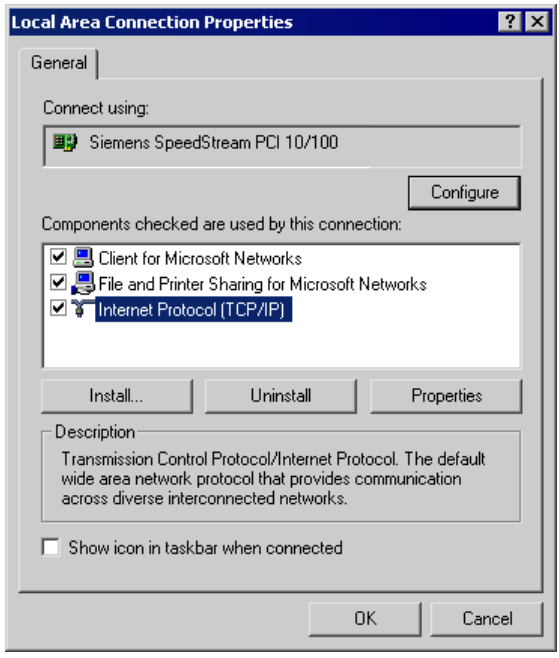


Figure 59: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

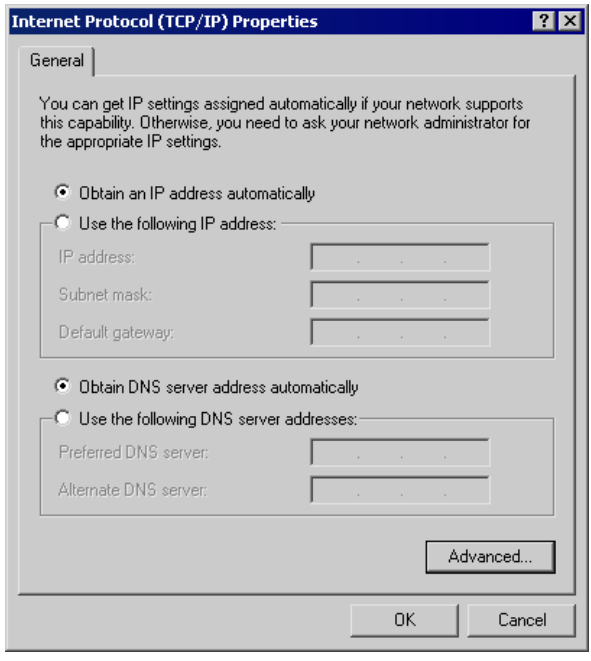

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 60: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. This is the default Windows settings. To work correctly, you need a DHCP server on your LAN.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

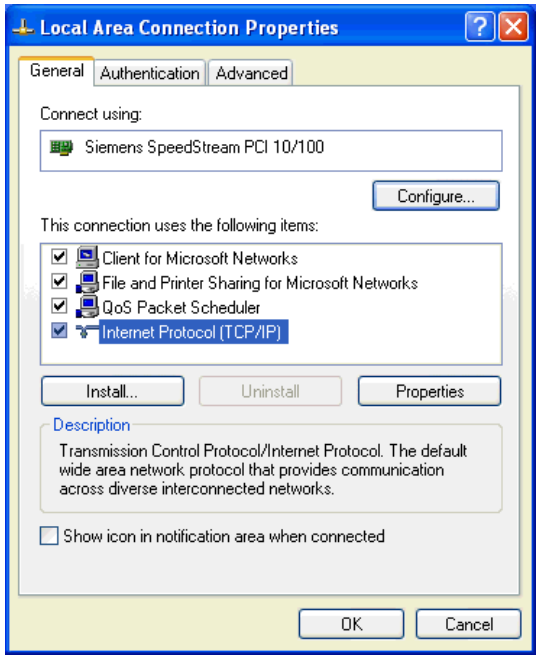


Figure 61: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

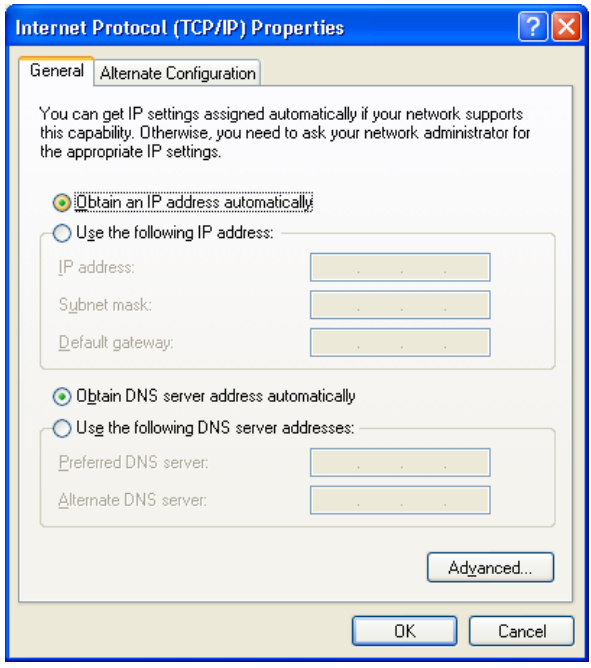

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 62: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. To work correctly, you need a DHCP server on your LAN.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Checking TCP/IP Settings - Windows Vista/7

1. Select Control Panel - Network Connections.
2. Right click the *Local Area Connection Status* and choose *Properties*. Click *Continue* to the *User Account Control* dialog box, then you should see a screen like the following:

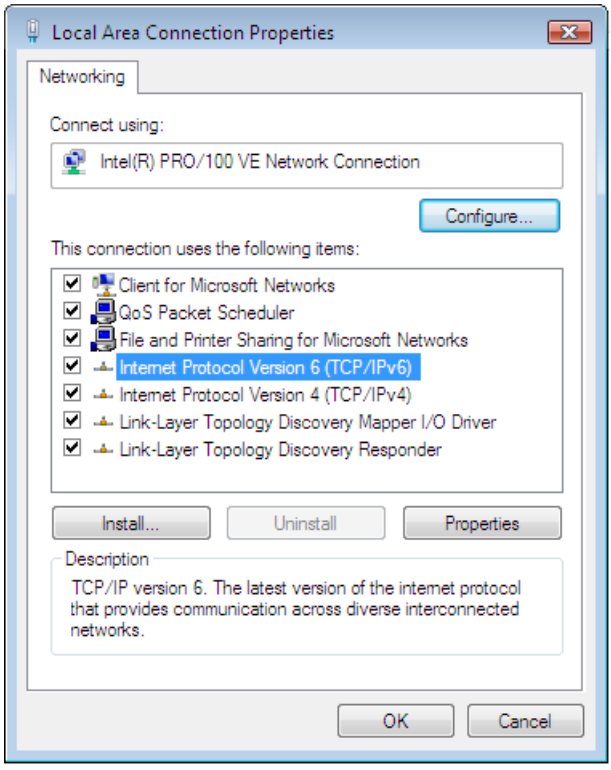


Figure 63: Network Configuration (Windows Vista/7)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

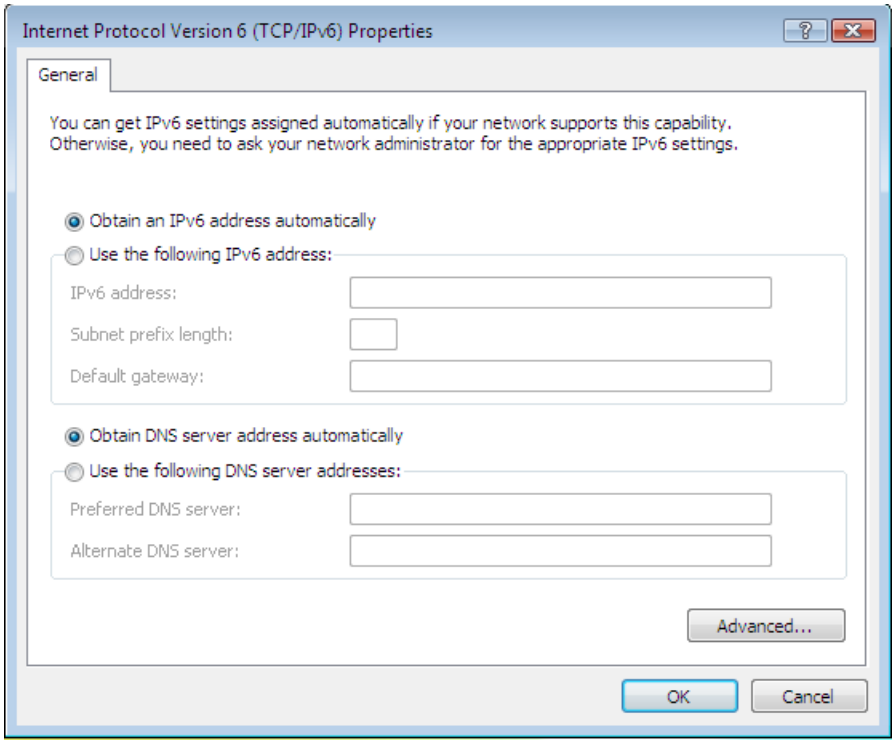

Internet Protocol Version 6 (TCP/IPv6) Properties
General
You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.
Obtain an IPv6 address automatically
Use the following IPv6 address:
IPv6 address:
Subnet prefix length:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 64: TCP/IP Properties (Windows Vista/7)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. To work correctly, you need a DHCP server on your LAN.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Appendix D
About Wireless LANs

Overview

Wireless networks have their own terms and jargon. It is necessary to understand many of these terms in order to configure and operate a Wireless LAN.

Wireless LAN Terminology

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

SSID/ESSID

BSS/SSID

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some Access Points allow connections from Wireless Stations which have their SSID set to “any” or whose SSID is blank (null).

ESS/ESSID

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. To reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. For 802.11g, 13 channels are available in the USA and Canada., but 11channels are available in North America if using 802.11b.
- If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference. The recommended Channel spacing between adjacent Access Points is 5 Channels (e.g. use Channels 1 and 6, or 6 and 11).
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Wireless Access Point must have the same settings.

WPA-PSK

Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.

WPA2-PSK

This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.

802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-Enterprise instead, because WPA encryption is much stronger than WEP encryption.

If this option is used:

- The Access Point must have a "client login" on the Radius Server.

- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.